macOS Support Essentials 10.14

Supporting and Troubleshooting macOS Mojave
Exam Preparation Guide

Contents

Becoming an Apple Certified Support Professional

The Apple Certified Support Professional (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 functions and that you can complete these tasks:

- Configure key services.
- Perform basic troubleshooting.
- Support multiple Mac users.

You must pass the macOS Support Essentials 10.14 exam in order to earn your ACSP certification. For more information, visit the Training and Certification website.

ACSP certification benefits

An ACSP certification is valuable because it differentiates you as a skilled user and support professional for macOS Mojave 10.14. You'll have the right to use the Apple Certified Professional logo on your résumé, business cards, and website. This certification gives you a competitive edge in today's evolving job market. It also enables you to benefit from the power of the Apple brand.

Before you take the certification exam, you must have (or create) an account in the Apple Certification Records System (ACRS). After you pass the exam, you'll 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. Then you can log in to ACRS and 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.

Preparing for the exam

The following exam preparation is recommended:

- Complete the macOS Support Essentials 10.14 course.

  Apple Authorized Training Providers (AATP) locations 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 Apple Pro Training Series book *macOS Support Essentials 10.14* by Arek Dreyer and Adam Karneboge.

  The Apple Pro Training Series book *macOS Support Essentials 10.14* 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.
  - 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.

  The best way to learn macOS technology is to use it. 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.

- Read this guide and practice completing the sample tasks and answering the review questions.

  You might be self-taught, or maybe you 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 this guide. 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.

- Consult some of the many third-party reference, troubleshooting, and online tutorials for users of various levels, from novice to power user.
- Post any questions you might have to the macOS Discussion Forum, hosted by Apple.

Exam details

The macOS Support Essentials 10.14 certification exam (no. 9L0-852) is a computer-based test offered at Apple Authorized Training Providers (AATP) locations. To find the closest AATP, visit the LearnQuest website. (LearnQuest is Apple's Global Training Provider.) If you don't see a session scheduled at your nearest AATP location, contact LearnQuest to find out whether a session can be scheduled for you. All AATP locations offer the macOS exam, even if they don't offer the corresponding course.

Here are the macOS Support Essentials 10.14 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 Exam and Certification FAQs webpage.
- You may not access any resources or references during the exam.
- Some exams are available in multiple languages. For details, visit the macOS Support Essentials 10.14 course page on the Apple Training website.

If you have questions about Apple certification exams, visit Exam and Certification FAQs.

Part One: Installation and Configuration

Lesson 1—Introduction to macOS

Goals

- Describe macOS.
- Describe new macOS Mojave 10.14 features.

Review questions

1. Which two industry standards have been shared with the developer community and have contributed to the success of macOS?
2. What is the default file system for all Mac computers running macOS Mojave?
3. What happens to the startup disk when you upgrade to macOS Mojave?
4. What are some of the new features of macOS Mojave?
5. Which four iOS apps are introduced with macOS Mojave?
6. Which privacy and security enhancements have been improved with macOS Mojave?
7. What is an upgraded function of Siri in macOS Mojave 10.14?
8. Where can you access a guided tour to learn about new macOS Mojave 10.14 features and learn how to navigate your Mac?

Answers

1. Multicast DNS for networking and the Swift programming language for writing software are two industry standards that have been shared with the developer community and have contributed to the success of macOS.
2. The default file system for all Mac computers is Apple File System (APFS).
3. The startup disk is automatically converted to APFS when you upgrade to macOS Mojave.
4. macOS Mojave new features include the following:
   - Dark Mode—A desktop look that helps you focus on your work.
   - Finder—An improved search feature that opens automatically. It displays at the top and bottom of the screen and stays open as you use other apps.
   - Stacks—A control-click feature that organizes and keeps your desktop clutter free.
   - Quick Actions—A feature that allows you to perform actions on a file, such as rotating an image or trimming audio or video clips, without opening the file.
   - Quick Look—A feature that allows you to preview the contents of many common file types, even without having apps installed.
   - Screenshot Utility—A feature that lets you capture a screenshot or record a screen when you press Shift-Command-5.
   - Continuity Camera—A feature that lets you import and scan your photos from your iOS device to your Mac and then insert them into a document.

5. The four apps introduced with macOS Mojave are listed below:
   - News
   - Stocks
   - Home
   - Voice Memos
6. macOS Mojave privacy and security enhancements include the following:
   - App permission requirements—An app must get consent before it can access the camera, microphone, or sensitive information such as location data, your message history, or your mail database.
   - Intelligent Tracking Prevention—It reduces the amount of information that sites can learn about your browser and device, and it limits an advertiser's ability to track you.
7. Siri can control your HomeKit-enabled devices, find your saved passwords, and discover more information about food, celebrities, and motorsports. It can even find your devices that are associated with your iCloud account and have Find My iPhone, Find My iPad, or Find My Mac turned on.
8. You can see a guided tour in the Finder when you select the Help tab. You have the choice of viewing:
   a. What's new in macOS?
   b. New to Mac? Tour the Basics.
   c. Get to know your MacBook Pro

Lesson 2—Update, Upgrade, or Reinstall macOS

Goals

- Describe the differences between a macOS update, upgrade, and reinstallation.
- Describe the macOS Installer.
- Update macOS.
- Upgrade macOS.
- Reinstall macOS.
- Verify system information
- Troubleshoot a macOS upgrade or reinstallation.

Review questions

1. What are the differences between a macOS update, upgrade, and reinstallation?
2. What steps should you take before you upgrade to macOS Mojave?
3. What are the system requirements to upgrade to macOS Mojave?
4. How do you check your Mac for updates?
5. How does the macOS installer know which firmware updates to download for your Mac?
6. How can you get the macOS installer?
7. How do you reinstall macOS?
8. What can you use to troubleshoot macOS installation issues?

Answers

1. The differences between a macOS update, upgrade, and reinstallation are listed below:
   - 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. This overwrites the existing system files but leaves apps, user home folders, and other files in place.
2. Before you upgrade to macOS Mojave, you should take these steps:
   a. Verify installation requirements.
   b. Plug notebook computers into power.
   c. Verify app compatibility.
   d. Back up important content.
   e. Document network settings.
   f. Open Software Update or the App Store.
3. The system requirements to upgrade to Mojave are listed below:
   - OS X Mountain Lion 10.8 or later
   - 2 GB of memory
   - 12.5 GB of available storage space for a new installation (or up to 18.5 GB of available storage to upgrade from OS X Yosemite 10.10 or earlier)
   - Compatible Internet service provider
   - Apple ID for some features
4. To check your Mac for updates, go to the App Store, click updates, and click the Update buttons for the App updates you want to install. Or you can Click the Update All button to install all of the updates.
5. The Installer uses your Mac model number to locate and download a firmware update specific for your Mac.
6. macOS installer is free and can be downloaded from the App Store.
7. To reinstall macOS, go to Utilities, select Install macOS, and continue to the license agreement. If it is acceptable, click agree, select your volume or show all disks, and select your volume and install.
8. To troubleshoot macOS installation issues from the macOS Installer menu bar, you can select the Window menu and then select and view the Installer Log.

Lesson 3—Set Up and Configure macOS

Goals

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

Review questions

1. Which tool guides you through the initial macOS Mojave configuration?
2. Which feature can significantly improve Apple ID security on Mac computers that have iCloud enabled?

3. Which key features do you gain by setting up iCloud?
4. Where can you manage iCloud settings after you configure macOS Mojave?
5. What's a configuration profile? How do you manage a configuration profile?
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 Mojave configuration process.
2. Two-factor authentication can improve Apple ID security if iCloud is enabled.
3. Key features of iCloud are that it provides cloud storage and communication services for apps, including iCloud Drive, Photos, Contacts, Calendars, Reminders, Safari, Siri, Notes, and Find My Mac. iCloud Keychain is also enabled if the Apple ID entered has two-factor authentication. If the Apple ID you entered belongs to the @mac.com, @me.com, or @icloud.com domain, Mail is also configured.
4. You can manage iCloud settings from iCloud preferences after you set up macOS Mojave.
5. A configuration 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 Mojave 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

- Describe when the command-line interface is useful.
- Use man pages to find more information about commands.
- Manipulate files in the command-line interface.

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 tasks?
   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 SSH protocol.
- Any administrator can run commands as the system administrator user or root, using sudo.
- The ability to automate repetitive tasks using scripting.
- The ability to remotely administer multiple, even thousands of Mac computers simultaneously using Apple Remote Desktop.

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. When are you prompted to enter a firmware password?
2. Which utilities are available when you start up from macOS Recovery?
3. What are the different macOS Recovery options and startup key combinations?
4. How can you create an external macOS installation disk?

Answers

1. You will see a prompt for a firmware password after you start your Mac up from macOS Recovery.

The firmware password prompt appears after you restart or turn on your Mac and then immediately press and hold Command-R. You release the keys when you see the Apple logo, a spinning globe, or the prompt for a firmware password.

2. macOS Recovery gives you access to Restore from Time Machine Backup, Install/Reinstall macOS, Get Help Online through Safari, Disk Utility, Startup Disk, Firmware Password Utility, Network Utility, Terminal, and Reset Password.
3. macOS Recovery installs different versions of macOS depending on the startup key combination you use:
   a. Command-R—Install the latest macOS that was installed on your Mac without upgrading to the latest version.
   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 or the version closest to it that is still available.
4. You can create a macOS Recovery disk that includes the macOS Mojave tools and installation assets with the `createinstallmedia` command-line tool in macOS Installer.

Lesson 6—Update macOS

Goals

- Configure automatic macOS software update settings in Software Update Preferences.
- Configure automatic App Store software update settings in App Store preferences.
- Automatically update Apple software.
- Manually update Apple software.
- Use an MDM solution to update macOS.

Review questions

1. Which apps does Software Update attempt to update?
2. What do you need to change Software Update preferences and the preferences in the App Store app?
3. How does macOS tell you that a software update is available from the App Store?
4. How does macOS tell you that a system update is available?
5. Which app should you open to initiate Apple software updates?
6. Which items are always installed, by default, through automatic software updates?
7. How can you control which software applications automatically update on a Mac?
8. Who can install system updates through the App Store?
9. Where can you find Apple software updates if you need to manually install an update?
10. What's the best way to learn what software is installed on a Mac?

Answers

1. macOS Software Update attempts to update this software:
   - Currently installed Apple software
   - macOS bundled software
   - Software you bought from the App Store

2. You need an Administrator account and the proper Apple ID to change Software Update preferences and the preferences in the App Store app.
3. For software updates, macOS displays an Updates Available notification in an alert with an App Store icon when updates are available and ready to be installed. In addition a red badge appears next to the App Store icon.
4. For system updates, macOS displays an Updates Available notification in an alert with a System Update icon. In addition, a red badge appears next to the System Preferences icon.
5. You should open the App Store app to initiate software updates.
6. System files and security updates are automatically installed, by default, when they’re available.
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. Users with administrator accounts can install system updates through the App Store.
9. You can find and download all Apple software updates at https://support.apple.com/downloads.
10. 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 Mojave? How are they different?
2. What other types of user accounts can macOS use in addition to local user accounts?
3. What are account attributes?
4. How can you limit a user account from having full access to all apps?
5. What does fast user switching allow you to do?

Answers

1. The local users accounts in macOS include the following:
   a. Administrator—Administrator user accounts are part of the admin group and are allowed full access to all apps, preferences, and shared resource locations.
   b. 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.
   c. Managed with parental controls—A managed account is a standard account with parental controls enabled.
   d. 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, such as preference files or web browser history.
   e. 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.
   f. System Administrator (Root User Account)—The System Administrator account has unlimited access to almost everything on a Mac. It is turned off by default on macOS.
   g. Group—A group account is a list of user accounts that gives you greater control over file and folder access.
2. There are two other user accounts in addition to the local user accounts that macOS uses:
   a. Network user accounts—Available to multiple Mac computers and is stored on a shared directory server such as Active Directory that centralizes identification, authentication and authorization information. The home folder for a Network user account is usually stored on a network file server.
   b. Mobile user account—A network user account that has been synced with the local user database so that you can use a mobile user account even when your Mac can’t contact the shared directory server. The home folder for a mobile user account is usually stored on the startup disk.
3. 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.

4. You can use parental controls to restrict what users can do.
5. 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

- 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. How do you turn on the Stacks feature to organize your desktop?
3. What is the default setting for the Library folder in the Finder?
4. Which folder can be used to share a file with another public user?
5. What options do you have when you delete a local user account?
6. What does Migration Assistant enable you to do?
7. 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. To turn on Stacks, click the Desktop to make the Finder the active app, and then from the View menu, choose Use Stacks. You can also Control-click the Desktop, then choose Use Stacks.
3. The Library folder is hidden in the default Finder view. The Library folder includes user-specific preference files, fonts, contacts, keychains, mailboxes, favorites, screen savers, and other app resources.
4. Every user has a Dropbox folder, located in their Public folder, which can be used to transfer files with other users. Users cannot add or make changes to files in your public folder.
5. 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.
6. 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.
7. 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

- Describe password types and use.
- Manage secrets in Keychain.
- Manage Secure Setup Utility.
- Enable and manage iCloud Keychain.
- Obtain User Approved MDM enrollment.
- Manage system-wide security and user privacy.
- Approve Kernel Extension Loading.

Review questions

1. What are the different types of passwords you use to secure a Mac?
2. What 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 iCloud Security Code?
8. Which three macOS functions require management of security-sensitive settings and enrollment with User-Approved MDM enrollment?
9. In what three ways can you obtain User Approved MDM enrollment?
10. Which macOS System-wide and personal settings can you manage in Security and Privacy?
11. Which feature can you enable to find a lost Mac?
12. How can you limit the use of Location Services?
13. How can you ensure that audio recordings used for Dictation service remain private?
14. Which three categories do kernel extensions (KEXTs) typically belong to?

Answers

1. The different types of passwords you use to secure a Mac are listed below:
   a. Local user account password—Used to log in to your Mac.
   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 from any disk other than your designated startup disk.
2. You use keychains to securely store resource passwords, certificates, keys, website forms, Safari AutoFill information, 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. Keychain files 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 they 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, such as your iPhone, iPad, or Mac.

7. iCloud Security Code is a separate technology used to further protect your secrets in iCloud Keychain. It is used when you enable iCloud Keychain with an Apple ID without two-factor authentication enabled. When two-factor authentication is not enabled, macOS prompts you to either enter or create your iCloud Security Code so you can trust the device. You can also use the iCloud Security Code to grant access to use your Apple ID on additional devices.

8. The following macOS functions require management of security-sensitive settings and enrollment with User Approved MDM enrollment:

   - Kernel extension loading policy
   - Autonomous single-app mode
   - User consent for data access

9. Three ways to obtain User-Approved MDM enrollment are listed below:

   a. Use Apple Business Manager or Apple School Manager to automatically enroll your Mac in an MDM solution. Its enrollment is equivalent to User Approved.

   b. Install macOS 10.13.4 or newer. If a Mac was enrolled in non-User Approved MDM before its update to macOS 10.13.4 or newer, it will be converted to a User Approved MDM enrollment.

   c. Follow the prompts in System Preferences to enroll in MDM. Download or email yourself an enrollment profile and double-click the enrollment profile.

10. macOS system-wide and personal settings that can be managed in Security and Privacy are listed below:

    a. General Settings—Provides the option to choose to require a password to wake a Mac from sleep or screen saver mode and to define a delay before this requirement sets in. Also allows you to configure a custom message to show at the login window or when the screen is locked.

    b. Advanced Settings—Provides the option to choose to require users to automatically log out of accounts after a certain amount of inactivity and to require an administrator password to access system-wide preferences

    c. FileVault Settings—Provides the option to enable and configure FileVault.

   d. Firewall Settings—Provides the option to enable and configure personal network firewall settings.

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

12. 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.

13. To ensure that your voice recordings remain private, you can manage your Enhanced Dictation settings manually. The Enhanced Dictation option is enabled by default. When you use Enhanced Dictation, your Mac immediately converts what you say into text without sending your dictated speech to Apple. If you turn Enhanced Dictation off or use Siri, then things you say and dictate will be recorded and sent to Apple to be converted to text. Along with this, Apple tracks other information such as your name, nickname, location and much of your user data sent from your device.

14. The three categories that kernel extensions (KEXTs) typically belong to are listed below:

   a. Low-level device drivers

   b. Network filters

   c. File system

Lesson 10—Manage Password Changes

Goals

- Change known passwords.
- Reset lost user passwords.
- Set a firmware password to secure macOS startup.
- Manage secure boot and external boot options for Mac computers that have the Apple T2 chip.

Review questions

1. How can you change your local computer account password?
2. How can you reset another user’s account password in macOS Mojave?
3. How does resetting a user’s account password affect that user’s login keychain?
4. When can you reset a login password with an Apple ID?
5. How can you reset a user’s lost account password if they can’t log in to their Mac?
6. How does Firmware Password Utility help prevent users from making unauthorized password changes?
7. Which two additional features are offered through Startup Security Utility to help secure unauthorized access for a Mac with an Apple T2 chip?

Answers

1. You can change your own local account passwords from the General pane of Security & Privacy preferences or from Users and Groups preferences. In either case, you select Change Password, and in the input pane, you must enter your old password once, followed by the new password twice. Finally, select Change Password.

2. You can reset other user account passwords if you have access to an administrator account on a Mac. To perform the reset from Users & Groups preferences you must authenticate as an administrator, select the user account you want to change, and select the Reset Password button. Then you must enter and verify the new password.

3. 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.

4. 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.

   You can do this in two ways:

   a. Enable FileVault and associate it with your Apple ID. Follow the proper steps and select “Reset it using Apple ID.”

   b. Restart your Mac in macOS Recovery. Follow the proper steps and select “I forgot my password.”

5. To reset a user’s lost account password, you can use the Reset Password assistant available from macOS Recovery along with the local user selection option.

6. The firmware password utility allows a user to turn on the firmware password, which prevents users who don’t have the password from starting up from any disk other than the designated startup disk.

7. Two additional features are offered through Startup Security Utility to help secure unauthorized access for a Mac with an Apple T2 chip. They are described below:

   a. Secure Boot—Ensures that your Mac starts up using only a legitimate and trusted version of an operating system (OS), including macOS or Microsoft Windows

   b. External Boot—Used to control whether your Mac with an Apple T2 chip can start up from an external hard drive, thumb drive, or other external media.

      The default and most secure setting is “Disallow booting from any external media.”

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. When should you use partitions instead of volumes?
3. What is the default partition scheme used by Mac computers?
4. Which major volume formats are supported by macOS Mojave?
5. What are some of the advantages of APFS?
6. What are the seven ways you can unmount and eject a volume or disk from the Finder?
7. Which two built-in macOS Mojave apps can you use to gather information about storage devices?
8. What does the Disk Utility First Aid feature do?

Answers

1. Formatting is the process of applying logic to storage in the form of partitions, containers, and volumes.
2. You should use partitions instead of volumes in these cases:
   a. You need to install multiple kinds of operating systems.
   b. You want to install Windows using Boot Camp Assistant.
3. GUID Partition Map (GPT)—This is the default partition scheme used by Mac computers.
4. macOS Mojave supports these major volume formats:
   - APFS— The macOS Mojave default.
   - Mac OS Extended—Used with and 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—Recent versions of Windows use this as their default native volume format. macOS can read but can't write to or start up from NTFS volumes.
5. APFS advantages are that it 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.

6. The seven methods you can use to unmount and eject a volume or disk in the Finder as listed below:
   a. Drag the disk icon to the Trash icon in the Dock.
   b. In the Finder sidebar, click the small Eject button next to the volume you want to unmount and eject.
   c. Select the disk you want to unmount and eject, go to the menubar, and choose File > Eject.
   d. Select the volume you want to unmount and eject, and then choose File > Eject *diskname*.
   e. Select the volume you want to unmount and eject, and then use the Command-E keyboard shortcut.
   f. Select the volume you want to unmount and eject, and then secondary-click (or Control-click) to reveal a pop-up menu enabling you to select Eject *diskname*.
   g. Select the disk you want to unmount and eject, click the Action button in the Finder window toolbar (it looks like a gear), and then choose Eject *diskname*.
7. Disk Utility and System Information can both be used to gather information about storage devices.
8. A Disk Utility First Aid feature is used to verify and repair the partition scheme and volume directory structures.

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. What are the differences between full-system encryption and full-disk encryption and the way that FileVault performs with each?
3. How can you turn on FileVault if you didn’t turn it on when you were prompted by Setup Assistant?
4. What are the two ways you can save the FileVault recovery key when you enable FileVault in Security & Privacy preferences?

Answers

1. FileVault encrypts the startup volume to protect user data.
2. The difference between full-system encryption and full-disk encryption and the FileVault requirements for each are listed below:
   - Full-System Encryption—Used in Mac computers with a T2 chip.

     Full-system encryption is automatic and integrates the function of several controllers that other Mac computers use. In this case, FileVault should be turned on for additional security, because without FileVault enabled, your encrypted SSDs will automatically mount and decrypt when connected to your Mac.
   - Full-Disk Encryption—Used in Mac computers without a T2 chip.

     FileVault uses full-disk encryption to help prevent unauthorized access to the information on your startup disk. FileVault performs the encryption at the file system driver level of macOS.
3. You can turn on FileVault at any time from Security & Privacy preferences.

4. FileVault Recovery offers two ways to recover passwords if FileVault passwords are lost:
   a. Use your Apple ID to unlock the FileVault volume and reset your password. This generates a random FileVault recovery key and saves it to your iCloud account on Apple servers.
   b. Record the key that FileVault randomly generates. You must keep the key letters and numbers somewhere safe and not on your encrypted startup disk.

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. Which ownership tiers are used with POSIX-style permissions to separately define specific privilege rules for each file and folder?
3. How do access control lists (ACLs) differ from standard UNIX file system permissions?
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. In Finder, you can open the Get Info window of each file or folder and find the permissions of each. Each file and folder has owner, group, and everyone permission settings.
2. The ownership tiers used with POSIX-style permissions to separately define specific privilege rules for each file and folder are listed below:
   a. Owner—By default, an item owner is the user who created the item or copied it to the Mac.
   b. Group—By default, the group permissions for an item are inherited from the folder it was created in.
   c. Everyone—Use the everyone permission settings to define access for anyone who isn't the owner and isn't part of the item's group.
3. Access control lists (ACLs) expand the standard UNIX permissions architecture to allow more file and folder access control. macOS has adopted a style of ACLs similar to what's available on Windows-based NTFS and UNIX file systems.
4. Every home folder contains a Public folder that other users can read and a Dropbox 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 enables local users to read and write files to it, but only the user who owns an item can delete it from the Shared folder. This folder's "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. Which two methods are used to hide items in macOS?
3. What is the difference between a package and a bundle?
4. What are the three primary file-system shortcut types that macOS uses?
5. How does an alias differ from a symbolic link?
6. Why would you use an archive file instead of a disk image? Why would you use a disk image instead of an archive file?
7. What type of file does the Finder create when you select the Archive option?
8. What action on macOS Mojave is set as the default for expanding the zip archive files?

Answers

1. The Finder hides certain folders —ones that contain resource items for macOS processes—from average users at the root of the system volume, because the average user doesn’t need access to those items. If you need access to these hidden files and folders you can use the Terminal.
2. You can hide items in macOS by using either of these methods:
   a. Use Terminal to add a period to the beginning of a filename.
   b. Enable the hidden file flag. (A hidden flag hides the items only in the Finder.)
3. The difference between a package and a bundle is described below:
   - A package—Any folder that the Finder presents to the user as if it were a single file.
   - A bundle—A folder with a standardized hierarchical structure that holds executable code and the resources used by that code.
4. The macOS file-system uses three primary shortcut types:
   a. Aliases
   b. Symbolic links
   c. Hard links
5. 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 is renamed or moved within the same volume. You can create an alias using the Finder, but it will not be recognized by Terminal. In contrast, any change to an original item breaks a symbolic link. You can create symbolic links only in Terminal, but the Finder follows symbolic links to an original item.

6. To differentiate why you would use a ZIP archive instead of a disk image or a disk image instead of a ZIP archive, here is the rationale:

   - For small amounts of data, you would compress files and folders into ZIP archives.
   - For larger data or the entire file system, you would create a disk Image.

   Additionally, 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 you can easily modify and convert them. Remember that macOS Mojave disk images can be accessed only by Mac computers; other systems require third-party software to access Mac disk images.

7. The Finder creates a compressed .zip archive file when you select the Archive option.
8. By default on macOS Mojave, double-clicking a .zip archive file causes the system to expand the contents of the .zip archive.

Lesson 15—Manage System Resources

Goals

- Explore and understand the macOS file layout.
- Discover common system files, their location, and their purpose.
- Describe System Integrity Protection.
- Manage font resources.

Review questions

1. What are the four default top-level folders that are 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. How does System Integrity Protection help ensure that macOS Mojave system resources remain secure?
6. Which app should you use to enable, disable, or validate a font or add a font to the local font library?
7. How can you identify duplicate fonts?

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. 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—Files that describe typefaces used for both screen display and printing. Font management is covered later in this lesson.

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. The four system resource domains and the purpose they serve is as follows:

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

6. You can use Font Book to enable, disable, or validate a font or add a font to the local font library.

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

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 Mojave?
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 should 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 allows you to quickly assign keywords, or "tags," to any item. A user can customize the tag names and colors and can create multiple tags for a single file.
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 issues 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.
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. How does Time Machine maintain a backup history of the file system?
3. Which types of files are omitted from Time Machine backups?
4. Why is Time Machine inefficient at backing up large databases?
5. What happens when you try to select an APFS volume as a Time Machine backup?
6. Which feature helps 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. 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. Software developers can also instruct Time Machine to ignore specific app data that does not need to be backed up.

3. 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.

4. If you select a backup disk that is formatted as APFS, FAT32, or any other file system besides HFS Plus, Time Machine offers to reformat it into the supported format of HFS Plus.

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.

Part Five: Applications and Processes

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. Which programs allow businesses and educational institutions to acquire multiple licenses for App Store items?
3. How many Apple IDs can be part of a Family Sharing group?
4. Where can you control access to the App Store and manage allowed apps for children?
5. From which two sources does macOS allow you to open apps?
6. Which security technologies does the Mac use to help protect users when they install third-party apps?
7. How do you install apps that aren't located in the App Store?
8. 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. The Apple Business Manager and Apple School Manager programs allow businesses and educational institutions to acquire multiple licenses for App Store items.
3. A Family Sharing group can have up to six members.
4. Parental Controls allows you to control your children's access to apps. The Apps tab lets you manage what apps your children access and prevent them from accessing the App Store. The Stores tab can be used to limit App Store purchases and available items based on age.
5. macOS allows you to open apps from the App Store and trusted developers. You can override this protection, however.
6. 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. System-wide 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—A warning appears 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.
   - Notarization—Indicates that Apple has performed a security check on the the software and no malicious software was found.

7. In addition to using the App Store, you can install software using drag-and-drop installations or installation packages.
8. 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 Autosave 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 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 are the built-in Quick Actions available in the Finder?
5. What's Autosave? How can you identify an app that supports Autosave?
6. How deep is the version history of a file that you share through email?
7. Which apps can manage document-locking?
8. Where should you adjust Autosave and Resume options? How should you disable Autosave?
9. What happens to your Home folder when you upgrade to iCloud Drive?
10. 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?
11. What happens to the user's Desktop & Documents folders if you disable iCloud Desktop & Documents?
12. What four Recommendations does Storage Management offer you for optimizing storage?

Answers

1. macOS Mojave 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 Mojave.
4. The list of actions available in Quick Actions depends on the kind of file or files you selected. Quick Actions includes these built-in actions:
   a. Rotate an image or movie—Rotate Left is the default command, but you can press and hold the Option key to change it to Rotate Right.

b. Mark up a document or image—After you choose Markup, the file opens in a Markup window. Read more about the Markup window in the next section.

c. Trim a movie or audio file—Choose Trim, then use the yellow handles in the trimming bar. Click Play to test your changes, then click Revert, or click Done to save your changes and close the window. After you click Done, macOS prompts you to replace your original file, cancel, or save your changes in a new clip.

d. Customize—Choose Customize to open the Extensions preferences in System Preferences.

5. Autosave allows compatible macOS Mojave 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 Autosave feature a Duplicate, Rename, or Move To command in the File menu.
6. Documents sent through email or otherwise copied to a shared location don't retain any version history.
7. Any app that supports Autosave and the Finder can manage document locking.
8. 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" to disable the Autosave feature for any app that supports it.

9. 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.
10. 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."
11. 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.
12. Recommendations for optimizing storage include the following:

- Store in iCloud—Store all files, photos and messages in iCloud and keep only recent files and optimized photos in local storage.
- Optimize Storage—Enable the removal of watched movies and TV shows in iTunes.
- Empty Trash Automatically—Automatically erase items that have been in the Trash for more than 30 days.
- Reduce Clutter—Sort through documents and other content stored on your Mac and delete what is no longer needed.

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 does app extensions add to macOS Mojave?
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 Mojave, what app do you use to examine open apps?
6. Which steps should you take when you troubleshoot app issues?
7. What are the three ways you can forcibly quit an app from the graphical interface?
8. What does the diagnostic reporting feature do?
9. Which file format is often used for preference files? How can you view the content of this file type?
10. Where are app preferences stored?

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 the 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. The three ways to forcibly quit an app from the graphical interface are as follows:
   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 or view it later in the /Applications/Utilities/Console app. It's reported to Apple through the Internet.
9. 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 Xcode, which you can get from the App Store.
10. 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.

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. How are IPv4 addresses constructed?
3. What's the purpose of Internet Protocol v4 (IPv4) addresses and subnet masks?
4. What is the default protocol macOS uses to get an IP address?
5. How does the IP transfer messages between computers over a wide area network (WAN)?
6. How is the Domain Name System (DNS) used to facilitate network naming?
7. What's used to identify a Wi-Fi network?
8. Which Wi-Fi authentication protocols are supported by macOS Mojave?
9. How can macOS Mojave 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. 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.
3. 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.
4. Mojave uses Dynamic Host Configuration Protocol (DHCP) to automatically acquire preliminary TCP/IP configuration and to assign IPv4 addressing.
5. 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.
6. The DNS is used to resolve a DNS name to the corresponding IP addresses.
7. A Service Set Identifier, or SSID, is used to identify a Wi-Fi network name and associated configuration.
8. macOS Mojave 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.

9. 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 Mojave?
3. How does network service order affect network connectivity?
4. How can you tell which interface is currently being used for network activities in Network preferences?
5. What's the easiest way to configure VPN settings in macOS Mojave?
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 Mojave 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. You can manually reorder your network service order list by selecting the Set Service Order under Network preferences and dragging them into your preferred order. Active services will still have priority over Inactive services.
5. The easiest way to configure VPN settings is to use a configuration profile containing all the relevant VPN setup information.
6. macOS Mojave 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. What is the term for the current data rate of a Wi-Fi connection, and where can you access this information about a specific Wi-Fi connection?
4. How can you verify basic connectivity to another network host?
5. How can you verify that DNS host name resolution is working?
6. 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 diagnostics 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 view the current data rate, or Tx Rate, of a selected Wi-Fi connection on the Wi-Fi status menu. The Wi-Fi status menu gives you access to important information about your connections and also allows you to access troubleshooting tools like Wireless Diagnostics. You can open the Wi-Fi status menu by pressing and holding the Option key and clicking the Wi-Fi icon in your menu bar.

4. 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.
5. You can use the Lookup tab in Network Utility to test name resolution against the currently configured DNS server.
6. 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 Mojave use dynamic network service discovery protocols to access network services?
5. Which two dynamic network service discovery protocols are supported by macOS Mojave?
6. Which five network file services can you connect to from the Finder "Connect to Server" dialog?
7. What is the default file-sharing protocol that macOS uses to connect a Mac that's running Mojave to another computer?
8. How are items inside the Finder Network folder populated?
9. In what two ways can you automatically connect a network share?
10. What are three common troubleshooting techniques you can use when you can't connect to network services?
11. 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 preferences is the primary interface in macOS Mojave for configuring built-in network apps, such as Mail, Calendars, Notes, reminders, Contacts, and Messages.
4. Some 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 Mojave 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. Bonjour is the primary set of dynamic network service discovery protocols used by macOS native services and apps.

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. Service Message Block (SMB) is the default, preferred file-sharing protocol used by MacOS Mojave.
8. 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.
9. 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.
10. Review Network preferences, review the Network Utility statistics, and try to connect to different network services.
11. 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 Mojave 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 Mojave?
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 Mojave, what are the firewall settings?

9. How does enabling stealth mode affect the way your Mac communicates with other hosts? How does blocking all incoming connections affect it?

Answers

1. The macOS Mojave 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 helps reduce Internet bandwidth usage and speed up software installation and iCloud content sharing on Mac computers, iOS devices, and AppleTV devices.

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

4. In macOS Mojave, 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 Mojave, 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 Mojave, the firewall settings are as follows:

- 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.

9. When stealth mode is enabled, your Mac doesn't respond to unauthorized network connections, including network diagnostic protocols like ping, traceroute, and port scan. Your Mac still responds to other allowed services. This includes Bonjour, which announces your Mac computer's presence and

prevents your Mac from being hidden on the network. When you block all incoming connections, your Mac won’t respond to incoming network connections except for those required for basic network services or established connections, such as those needed to browse the web or check email. This prevents shared services or apps hosted on your Mac from working remotely.

Part Eight: System Management

Lesson 26—Troubleshoot Peripherals

Goals

- Manage peripheral connectivity.
- Pair Bluetooth devices with 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 Mojave?
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 Mojave 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. The four primary peripheral bus technologies supported by macOS Mojave are as follows:
   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 Mojave and a peripheral. The three primary types of device drivers are as follows:
   a. Kernel extensions
   b. Framework plug-ins
   c. Standalone apps
4. macOS Mojave 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. Which Apple technology helps you find printers and print without downloading or installing printer drivers?
2. What does the CUPS do?
3. How can you select a new printer driver for a configured printer?
4. Which two actions might you need to take to find and connect a Windows-based computer to your CUPS-shared print service?
5. Under what circumstances can a standard (nonadministrative) user configure a printer?
6. How do you share printers with other users?
7. How does sleep mode affect users' access to shared print services?
8. How do you create a PDF document?
9. What are the three ways you can access a printer queue app?
10. What's a potential quick fix if it appears that a configured printer has a problem?

Answers

1. AirPrint.
2. CUPS manages printing for macOS Mojave, including local and shared printing.
3. 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.
4. The CUPS-shared print service allows network clients to locate your shared printer configurations using Bonjour. However, different versions of Windows might require you to add additional drivers. Network clients can also enter your Mac computer's IP address or DNS host name to access your Mac shared print service.
5. Assuming the default settings for macOS Mojave, 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.
6. Users cannot access shared print services on a Mac in sleep mode. To ensure that sleep mode does not interfere with shared printing, you can either disable your Mac computer's automatic sleep activation or enable "Wake for Wi-Fi network access" from Energy Saver preferences.
7. You can enable printer sharing from Print & Scan or Sharing preferences.
8. In any Print dialog, click the PDF button. You can then choose one of the options in the pop-up PDF menu to save or send the new PDF file.
9. If a printer queue is open, you can click its icon in the Dock. If the printer queue disappears from the Dock before you can click it, you can open Printers & Scanners preferences, select the queue on the

left, and click Open Printer queue. You can also manually open a printer queue from the Finder by navigating to ~/Library/Printers, and then double-clicking a printer.

10. 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 is the role of the T2 chip in a macOS Mojave startup?
2. What happens if your macOS with a T2 chip identifies errors and experiences failures during the secure startup process?
3. What are the primary system initialization stages in macOS Mojave? What visual and audible cues do these stages provide?
4. What does the firmware do? What's the Power-On Self-Test (POST)?
5. What role does `launchd` serve during Mac startup?
6. Which items are automatically started by `launchd` during Mac startup?
7. What are the primary user session stages in macOS Mojave? What visual and audible cues do these stages provide?
8. What's the difference between launch daemons, startup items, launch agents, and login items?
9. What are Safe Sleep, Standby, and Power Nap?
10. What happens during user logout?
11. What happens during Mac shutdown?
12. Which keyboard shortcut is used to start up in safe mode?
13. Which keyboard shortcut can you temporarily use to choose another startup disk?
14. What changes are made when macOS Mojave starts up in safe mode?
15. Which items aren't loaded when macOS Mojave starts up in safe mode?

Answers

1. The T2 Chip verifies every step of the boot process to ensure that the hardware and software haven't been tampered with.
2. If your macOS with a T2 chip identifies errors and experiences failures during the secure startup, then your Mac will enter macOS Recovery, Apple T2 Security Chip recovery mode, or Apple T2 chip Device Firmware Upgrade mode.
3. Each primary stage of system startup can be indicated by the following cues:
   a. Firmware—Power on. Power On Self Test (POST). Startup Chime (depending on model).
   b. Booter—The booter process starts. The Apple logo appears in the center of the main display.
   c. Kernel—Kernel startup. The progress bar appears.
   d. System `launchd`—Starting other items. The Apple logo is replaced with the login window.
4. 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.

5. `launchd` starts macOS Mojave processes. It also manages macOS Mojave initialization and starts the loginwindow process.

6. During macOS Mojave startup, `launchd` starts these daemons and scripts:

- /System/Library/LaunchDaemons
- /Library/LaunchDaemons

7. Each primary stage of a user session can be indicated by the following signs:

   a. The login screen appears.

   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 Mojave.

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

9. Safe Sleep and Standby are modes used by Mac computers that use very little or no power to safeguard data. When Mac computers go to sleep, they copy the entire contents of system memory to an image file on the system volume. This way, if your Mac stays in sleep mode long enough to completely drain the battery, no data is lost when your Mac has to turn off.

- Safe Sleep—Your Mac enters this mode if the battery becomes completely drained or if you leave your Mac idle for a long time. To wake your computer, restart your Mac just like it was shut down. All Mac models compatible with macOS Mojave support this mode.
- Standby—Your Mac enters this mode as a power-saving standby when it is asleep and completely idle for more than 1 hour, or after 3 hours, depending on the manufacture date. To wake your Mac, interact with the keyboard, trackpad or mouse; you don't need to restart your computer. This mode is used by newer Mac computers with flash storage.

Power Nap is a state that periodically runs updates while your computer is sleeping.

- Power Nap—Information is periodically updated on your Mac while is sleeping. The type of information that is updated varies, depending on whether your Mac is running on battery power or plugged into a power adapter. Power Nap enablement varies by type of computer.

10. 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

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

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

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

14. 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

15. When macOS Mojave 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.