Lesson review questions summarize what you’ve learned in each lesson and help you prepare for the Apple certification exam.

**Lesson 1 Review**

There are no review questions for Lesson 1.

**Lesson 2 Review**

1. What are the minimum hardware requirements for upgrading a system with OS X Mountain Lion?
2. What four preparation steps must you take before upgrading a system with OS X Mountain Lion?
3. How can you identify if a Mac requires a firmware update?
4. What are the advantages and disadvantages of using a single-partition disk with OS X? How about a multiple-partition disk?
5. How can you acquire the OS X Mountain Lion installation assets?
6. What options can you select from during the OS X Mountain Lion installation?

**Answers**

1. The minimum requirements for upgrading OS X Mountain Lion are:
   - OS X v10.6.8 or later
   - 2 GB of memory
   - 8 GB of available space
   - Some features require an Apple ID.
   - Some features require a compatible Internet service provider.
   - A compatible Mac model as listed at www.apple.com/osx/specs/
2. Four steps you should take before upgrading a system to OS X Mountain Lion are: install Apple software and firmware updates, verify application compatibility, back up important files and folders, and document critical settings.

3. You can identify a Mac computer’s firmware version by opening the full system report in the System Information application or System Profiler application. You can verify if a Mac computer’s firmware is up-to-date by visiting the Apple support website, which maintains a list of available firmware updates.

4. Single-partition drives are easier to set up initially, but they aren’t as flexible for administration and maintenance. Multiple-partition drives require repartitioning during setup but provide several separate partitions, which can be used to segregate user data and host multiple operating systems.

5. The OS X Mountain Lion installer can only be purchased and downloaded from the Mac App Store.

6. During installation of OS X Mountain Lion, the only optional choice is to define an installation destination other than the Mac computer’s current default system disk.

Lesson 3 Review

1. What key features do you gain by setting up iCloud?

2. What three primary sources can Migration Assistant pull from?

3. What are the five System Preference categories?

4. How do the four default System Preferences categories differ?

5. What is a configuration profile? How are they managed?

6. Where can you locate the system version number, build number, and serial number? What is the significance of these numbers?

Answers

1. iCloud is a free service from Apple that provides cloud storage and communication services for applications, including Mail, Contacts, Calendars & Reminders, Notes, Safari, Photo Stream and any other applications that support iCloud integration. iCloud also provides Find My Mac technology for help locating a lost or stolen system.

2. Migration Assistant can migrate information from other OS X systems, other Windows systems, and other disks, including Time Machine backups.

3. System Preferences is divided into five categories, from top to bottom; Personal, Hardware, Internet & Wireless, System, and Other.
4. Generally, Personal preferences affect only a single user; Hardware preferences adjust hardware and peripheral settings; Internet & Wireless preferences affect personal and system network settings; and System preferences affect all users and often require administrative access.

5. A configuration profile is a document, with the filename extension “.mobileconfig,” that contains system settings as defined by an administrator. Opening a configuration profile will prompt the system to install the profile and configure the settings. Installed configuration profiles can be managed via the Profiles preference.

6. The system version, build number, and hardware serial number are located in the About This Mac dialog or the login screen. The system version number defines the specific version of OS X currently installed. The system build number is an even more specific identifier used primarily by developers. Finally, the hardware serial number is a unique number used to identify your specific Mac.

**Lesson 4 Review**

1. What utilities are available when started up from OS X Recovery?

2. What two resources does the local hidden OS X Recovery HD need in order to reinstall OS X Mountain Lion?

3. What two methods can be used to create an external OS X Recovery disk?

**Answers**


2. The local hidden OS X Recovery HD does not include the OS X installation assets. Thus, reinstalling OS X Mountain Lion from here requires high-speed Internet access and the ability to verify access to the installation assets. Upgraded Macs are verified by entering the Apple ID used to purchase OS X Mountain Lion. Conversely, verification is automatic for Macs that included OS X Mountain Lion.

3. The OS X Recovery Disk Assistant can create a minimal OS X Recovery disk. A full OS X Recovery disk can be created by using Disk Utility to copy the Install OS X Mountain Lion application assets to the disk.
Lesson 5 Review

1. Which application can you open to initiate Apple software updates?
2. By default, are any items automatically installed via Apple software update?
3. Which applications are used to manually acquire and install OS X software updates?
4. How can you find which installations have taken place on the system?

Answers

1. All software updates are handled via the Mac App Store.
2. Important system files and security updates are automatically installed after a period of several days.
3. OS X software updates can be downloaded from the Apple support website using any modern web browser. Updates take the form of installation packages that are installed via the Installer application.
4. The Installations section of System Information will show the history of all software installed via the Mac App Store or the OS X Installer.

Lesson 6 Review

1. What are the five types of user accounts in OS X? How are they different?
2. What are some security risks associated with each type of user account?
3. What are account attributes?
4. How can you limit a user account from having full access to all applications?
5. What types of resource contention issues can occur when fast user switching is enabled?
6. What security risk related to storage can occur when fast user switching is enabled?

Answers

1. Standard is the default account type; administrative users can make changes to the system; a guest user does not require a password; sharing only users can access only shared files; and the root user has unlimited access.
2. Standard user accounts are very secure, assuming they have good passwords. Administrative users can make changes that may negatively affect the system or other user accounts. A guest user could potentially fill shared folders with unwanted files. Sharing
only users are generally very secure as long as you don’t give them too much access to your items. The potential for mayhem with root user access is nearly unlimited.

3. Account attributes are the individual pieces of information used to define a user account. Examples include full name, account name, user ID, Universally Unique ID (UUID), group, and home folder.

4. Parental controls can be used to further limit a user account. Examples include enforcing a simple Finder, limiting applications and widgets, setting time limits, and content filtering for several applications included in OS X.

5. Resource contention occurs when fast user switching is enabled and a user tries to access an item another user already has open in the background. Document contention occurs when a user attempts to open a document another user has already opened. Peripheral contention occurs when a user attempts to access a peripheral already in use by another user’s open application. Application contention occurs when the second user attempts to access an application designed to run only once on a system.

6. When fast user switching is enabled, all users are allowed to see other users’ locally connected disks.

Lesson 7 Review

1. What default folders make up a user’s home folder? What are some optional folders in a user’s home folder?

2. When deleting a local user account, what three options does the User & Groups preference give you for dealing with the user’s home folder content?

3. How do you make OS X associate a new local user account with a manually migrated or restored user’s home folder?

Answers

1. The default folders in a user’s home folder are Desktop, Documents, Downloads, Library (hidden), Movies, Music, Pictures, and Public. Optional home folder items include Applications and Sites folders.

2. When deleting a local user account OS X can archive the home folder content into a compressed disk image, leave the home folder content in the /Users folder, or delete the home folder content. Optionally, OS X can perform a secure erase on the home folder content.
3. Before the local user account is created on a system, you must first copy the restored user’s home folder to the /Users folder. Then once you create the new user in the Users & Groups preference with the same account name, the system will prompt you to associate the new account with the restored home folder.

**Lesson 8 Review**

1. What does the master password do?
2. What methods can be used to reset a user’s lost account password?
3. How does a user that changes his own account password affect his login keychain?
4. How does resetting a user’s account password affect that user’s login keychain?
5. How does resetting the master password affect existing Legacy FileVault user accounts?
6. How can you limit the use of Location Services?
7. What can you enable to locate a lost Mac system?
8. How does the Firmware Password Utility help prevent users from making unauthorized password changes?

**Answers**

1. The master password can only be used to reset local account passwords.
2. Local account passwords can be reset by an administrator in Users & Groups, the master password at login, an Apple ID at login, a FileVault 2 recovery key at startup, and by the Reset Password application in OS X Recovery.
3. When a user changes his own account password, the system will keep his login keychain password in sync.
4. Any account password reset process will not change any keychain passwords. Therefore, the user’s keychains will not automatically open when the user logs in with her new password. The user will have to manually change her keychain passwords using the Keychain Access utility.
5. If a master password is reset because it was lost, Legacy FileVault accounts cannot be reset by the new master password.
6. The Privacy pane of the Security & Privacy preferences can be used to verify or disable applications’ access to Location Services and other personal information.
7. iCloud Find My Mac allows you to remotely locate a lost Mac or iOS device.
8. The Firmware Password Utility prevents users from starting up from another system disk. This in turn prevents them from using an OS X Recovery system to reset local passwords without authorization.

**Lesson 9 Review**

1. What type of items can be found in a keychain?
2. How does the keychain system help protect your information?
3. Where are the keychain files stored?
4. What application is used to manage keychain settings?

**Answers**

1. Keychains are primarily used to store authentication secrets such as resource passwords, digital certificates, and encryption keys. The keychain system can also securely store website form information and text notes.

2. The keychain system manages encrypted files that are used to securely save passwords, certificates, or notes. By default, every user has a login keychain that has the same password as his account. Not even other administrative users can access your keychain secrets without knowing the keychain's password.

3. Each user starts with a default login keychain at /Users/<username>/Library/Keychain/login.keychain, and they can store other keychains in the same folder. Administrative users can manage systemwide authentication assets with the /Library/Keychain/System.keychain. Finally, Apple maintains several items in /System/Library/Keychains/ for OS X system use.

4. Keychains can be managed from the /Applications/Utilities/Keychain Access application.

**Lesson 10 Review**

1. What is the difference between disks, partitions, and volumes?
2. What are the two primary partition schemes for Mac-formatted disks? What are their differences?
3. What two volume formats are supported for an OS X system volume?
4. How does file system journaling work?
5. What are the four erase options available in Disk Utility? What are the differences between them?
6. How does the Secure Empty Trash feature in Finder work?
7. How can you ensure that previously deleted items are securely erased?
8. How can you encrypt a disk without erasing its contents.
9. What four methods can be used to eject a volume or disk from the Finder?
10. What is the potential side effect of improperly unmounting or ejecting a disk or volume?

**Answers**

1. Disks are the actual storage hardware; partitions are logical divisions of a disk used to define the storage space; and volumes, contained inside partitions, are used to define how the individual files and folders are saved to the storage.

2. GUID Partition Table is the default partition scheme on Intel-based Macs, and Apple Partition Map is the default partition scheme on PowerPC-based Macs.

3. The volume formats supported as system volumes for OS X are Mac OS Extended (Journaled) and Mac OS Extended (Journaled, Encrypted).

4. File system journaling records what file operations are in progress at any given moment. This way, if a power failure or system crash occurs, after the system restarts it will be able to quickly verify the integrity of the volume by “replaying” the journal.

5. The four erase options in Disk Utility are Fastest, which simply replaces the volume’s directory structure; a second choice, which provides good security by writing zeros on top of all the previous disk data; a third choice, which provides even better security by writing three separate passes of information on top of the previous disk data; and Most Secure, which provides the best security by writing seven separate passes of information on top of the previous disk data.

6. Secure Empty Trash will perform a 7-pass erase on the contents of the Trash folder.

7. From the Erase tab in Disk Utility, you can choose to securely erase the free space of a disk or volume. This securely erases any previously deleted files on the selected disk or volume.

8. From the Finder you can encrypt a disk without erasing its contents by secondary (or Control) clicking the disk and then choosing Encrypt from the shortcut menu.

9. The four methods used to eject a volume or disk from the Finder are to drag the disk icon to the Trash in the Dock; press and hold the Eject key for a few moments to unmount and eject optical media; select the volume you want to unmount and eject from the Finder and choose File > Eject; and, finally, in the Finder sidebar, click the small Eject button next to the volume you want to unmount and eject.
10. Improperly unmounting or ejecting a drive or volume may cause data corruption. The system automatically verifies and repairs an improperly unmounted or ejected volume the next time it becomes available to the Mac.

**Lesson 11 Review**

1. How does FileVault 2 protect a user’s data?
2. What are the system requirements for using FileVault 2?
3. Which users are allowed to unlock a FileVault 2 protected system?
4. How can you unlock a FileVault 2–protected system when all user accounts have lost their passwords?

**Answers**

1. FileVault 2 protects the entire system volume and all its data by using strong XTS-AES 128 encryption. During system startup, a FileVault-enabled user must enter her password to decrypt the system volume.

2. To enable FileVault 2, OS X systems must have the hidden OS X Recovery HD volume on the system disk. Further, any Legacy FileVault accounts must be decrypted and returned to normal accounts.

3. Any user that is FileVault enabled is allowed to unlock a FileVault 2–protected system. This includes any local or cached network user account that was enabled when FileVault 2 was set up or created after FileVault 2 was enabled. Further, administrators may return to the Security & Privacy preference to enable additional accounts.

4. A FileVault 2 protected system can be unlocked using the recovery key that was generated during the FileVault 2 setup process. This key can be entered during system startup, and will allow you to reset the user’s account password.

**Lesson 12 Review**

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. What is the locked file flag?
4. Why is the root, or beginning, level of a user’s home folder visible to other users?
5. How does the default organization of the file system allow users to safely share local files and folders?
6. What is unique about the permissions of the /Users/Shared folder?

7. What does it mean when you choose the option to “ignore volume ownership” in the Finder? What are the security ramifications of ignoring volume ownership?

**Answers**

1. An item's ownership and permissions can be identified using the Get Info or Inspector windows in the Finder.

2. Standard UNIX file system permissions allow only for permissions to be set for one owner, one group, and all others. ACLs, on the other hand, allow for an essentially unlimited list of permissions entries.

3. The locked file flag prevents anyone, including the item's owner, from editing an item. Only the item's owner can unlock the item to then allow modification.

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

5. 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 do not allow access to other users. The Shared folder is also set for all users to share items.

6. 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. This is accomplished using the sticky bit permissions setting.

7. You can choose to ignore ownership on any nonsystem volume. This will ignore any ownership rules and grant any logged-on user unlimited access to the contents of the volume. It is a potential security risk because it will allow any local user account to have full access to the volume even if that user did not originally mount the volume.

**Lesson 13 Review**

1. Which two built-in OS X applications can be used to gather information about storage devices?

2. What does the Disk Utility Verify and Repair feature do?

3. What is target disk mode and how is it engaged?

4. What permissions are modified by the Disk Utility Repair Permissions feature?

5. How can you reset a user's home folder permissions?
Appendix A: Lesson Review Questions and Answers

Answers

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

2. The Disk Utility Verify and Repair feature is used to verify or repair the partition scheme and directory structure of a volume. These elements contain the information used to locate files and folders on the volume.

3. Target disk mode is a Mac-specific hardware feature that, when engaged, will share the Mac computer’s internal disk disks through the FireWire ports. Target disk mode can be engaged from the Startup Disk preferences or by holding down the T key as you turn on the Mac.

4. The Disk Utility Repair Permissions feature repairs only the ownership and permissions for items installed by Apple. However, this may resolve issues with third-party products.

5. A user’s home folder permissions can be reset from the Reset Password application on OS X Recovery.

Lesson 14 Review

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 OS X use bundles or packages for?

4. How does an alias differ from a symbolic link?

Answers

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

2. The Finder does not show items with periods at the beginning of their filenames or items with the hidden file flag enabled. Neither method can be accidentally enabled using the Finder or default OS X applications.

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 through deletion or moving of 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 should it be renamed or moved within the same volume. Whereas, any change to an original item breaks a symbolic link.

Lesson 15 Review

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? Where are they located in the file hierarchy?
3. What are the four system resource domains? What purpose does each domain serve?
4. What happens when a user double-clicks a font file?
5. How can you identify duplicate fonts?

Answers

1. The four default top-level folders visible in the Finder are Applications, containing applications all local users have access to; Library, containing system resources all local users have access to; System, containing necessary system resources; and finally, Users, containing all the local user home folders.

2. Six common system resources are extensions, which attach themselves to the system kernel to provide hardware and peripheral driver support; frameworks, which are shared code libraries that provide additional software resources for both applications and system processes; fonts; preference files, which contain application and system configuration information; LaunchAgents and LaunchDaemons, used by launchd to provide services that automatically start when they are needed, at system startup, or at user login; and finally, logs, which are text files that contain error and progress entries from nearly any application or system service.

3. The four system resource domains are User, containing applications and system resources specific to each user account; Local, containing applications and system resources available to all users on the local Mac; Network (optional), containing applications and system resources available to any Mac that has an automated network share; and finally, System, containing applications and system resources required to provide basic system functionality.

4. Double-clicking a font file automatically opens a preview of the font in the Font Book application. From here the user can click the Install Font button to copy the font into ~/Library/Fonts.
5. The Font Book application shows a small dot next to the name of any font that has duplicate resources.

Lesson 16 Review

1. What is file system metadata? What are some examples of file system metadata?
2. What are some of the common file flags used by OS X?
3. How does the Spotlight search service use metadata?
4. Where does Spotlight store its metadata index databases? How about the Spotlight plug-ins?
5. What are some privacy and security concerns with the Spotlight service?
6. How do you resolve an issue where a Spotlight search doesn’t appear to be finding the correct items?

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. The Spotlight search service creates index databases of file system metadata so that it can perform normally time-intensive searches nearly instantly.

4. 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 his encrypted home folder. Also, the Mail application 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.

5. Though Spotlight indexes file and folder permissions, it allows other users to search the contents of locally attached nonsystem volumes when ownership is ignored on those volumes.

6. Forcing a rebuild of the Spotlight index databases is a common technique to resolve search issues. You can force a rebuild by adding an item to the Spotlight preferences Privacy list, and then removing the item. This deletes the current index database and forces the system to build a new one.
Lesson 17 Review

1. What type of file is created by the Finder when you select the Archive option?
2. What OS X application is set as the default for opening archive files?
3. Which OS X application is responsible for the creation and management of disk images?
4. Why would one use an archive file over a disk image? Why would one use a disk image over an archive file?

Answers

1. The Archive option in the Finder creates compressed zip archive files.
2. By default on OS X, double-clicking a zip archive causes the system to expand the zip archive into a folder next to the same location as the original zip archive.
3. Disk Utility is the primary application for creating and managing disk images.
4. 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, disk images can be easily modified and converted. However, OS X style disk images are not compatible with third-party operating systems.

Lesson 18 Review

1. What backup destination disks does Time Machine support?
2. How does Time Machine maintain a backup history of the file system?
3. What types of files are omitted from Time Machine backups?
4. Why is Time Machine inefficient at backing up large databases?
5. Why might a previously backed-up item no longer be available in Time Machine?
6. What four methods can be used to restore from a Time Machine backup?

Answers

1. Time Machine can back up to any Mac OS Extended volume, or network shares hosted from Time Capsule or OS X Server.
2. Time Machine starts with a full copy of the file system to the backup disk. Then it maintains a list of changes to the file system, and every hour copies only the changes to the backup disk. In the backup it creates a simulation of the full file system using hard links for files that have not changed.
3. Time Machine always ignores temporary files, Spotlight indexes, items in the Trash, log files, and anything else that can be considered a cache. Time Machine also ignores any files an application has defined as exempt, or any files you have defined as exempt in the Time Machine preferences.

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 will not be available if your backup volume filled up and Time Machine had to start deleting older items to make room for newer items.

6. Methods for restoring from a Time Machine backup include navigating through the backup history via the Time Machine application; restore a user account via Migration Assistant; restore an entire system via OS X Recovery; or manually restore items via the Finder.

Lesson 19 Review

1. What are the requirements for purchasing applications via the Mac App Store?

2. In the Mac App Store, how can you verify which Apple ID is currently being used for purchases?

3. What are the four primary application environments supported by OS X? Which ones require an additional download and installation?

4. What are the advantages of application sandboxing?

5. What are the advantages of code signing?

6. Which items fall under the file quarantine system?

7. What three security options does the Gatekeeper system allow? Which Gatekeeper option is the OS X default?

8. What are the two primary traditional installation methods in OS X?

9. What three methods can be used to uninstall applications?

Answers

1. The requirements to purchase items from the Mac App Store are OS X v10.6.6 or later, an Apple ID, an Internet connection, and authorization as a local administrator.

2. In the Mac App Store, you can view the current Apple ID by selecting Store from the menu bar. You can get further details regarding this Apple ID, by selecting View My Account in the same menu.
3. The four primary application environments supported by OS X are native OS X applications, which are created using Cocoa or Carbon; UNIX applications, which are primarily accessed via Terminal; Java applications, which work as cross-platform applications; and X Window System applications, which is a popular UNIX windowing environment. OS X does not include the Java application or X Window System runtime, so they must be downloaded and installed after the OS X initial installation.

4. Sandboxed applications are only allowed access to specific items. They are otherwise completely cut off from the rest of the system, and are therefore unable to cause undue harm. All Mac App Store applications are required to be sandboxed.

5. Code-signed items include a digital signature that the system can use to verify the authenticity and integrity of the application or process and its resources.

6. Any item downloaded using one of the built-in OS X applications will be marked for quarantine. Third-party applications may not mark downloaded items for quarantine.

7. Gatekeeper can restrict software to Mac App Store applications only, or Mac App Store and identified developer applications only (this is the default option), or any application regardless of origin.

8. Traditional installation methods are generally categorized as either a drag-and-drop installation, where the user simply copies the application to the local system; or as an installation package, where an installer process places the items on the local system.

9. Three methods for uninstalling applications include opening Launchpad, holding the Option button, and then clicking the “X” button; in the Finder drag the primary application to the Trash and then empty the Trash; and most rarely opening a custom-built uninstaller package.

Lesson 20 Review

1. In OS X what is used to identify the type of application that should open when you double-click a document?

2. How do you engage Quick Look? Which applications support it?

3. How is Quick Look able to preview so many file types?

4. What is Auto Save? How can you identify an application that supports Auto Save?

5. How deep is the version history of a file when shared via email?

6. Which applications can manage document locking?

7. What interface is the default location for managing documents in iCloud?

8. Where can you adjust application resume options?
Answers

1. OS X uses a document’s filename extension to determine the document’s type. The Launch Services process maintains a database of installed applications and which document types they are capable of opening.

2. Quick Look is engaged by simply pressing the Spacebar when a document is selected. Applications that support Quick Look include Finder, Time Machine, Mail, and most open and save browser dialogs.

3. Quick Look uses a number of plug-ins that give it the capability to preview documents. These plug-ins live in Quick Look folders in any Library folder on OS X.

4. Auto Save is a new feature in OS X that allows applications to automatically save changes to users’ documents. Once the user saves a document the first time, he never has to think about saving changes again. Applications that support Auto Save feature a Duplicate function in the File menu as opposed to a default Save As function.

5. Documents sent via email or otherwise copied to a shared location do not retain any version history.

6. Any application that supports Auto Save and the Finder can manage document locking.

7. Documents saved to iCloud can be managed from the application that was used to create and save the document. iCloud documents do not appear anywhere in the Finder a user would normally look.

8. You can manage “application resume after log out” options from the logout verification dialog. You can manage “application resume after quit” options from the General preferences.

Lesson 21 Review

1. What is protected memory? What is 64-bit memory addressing?

2. Why would you want to open an application in 32-bit mode?

3. How can you identify the type of a particular application?

4. How can you identify which applications are installed on your Mac?

5. Which application is used to examine open applications on OS X?

6. What steps should you use when troubleshooting application issues?

7. What three ways can you forcibly quit an application from the graphical interface?
8. What does the diagnostic reporting feature do?

9. Where are application preferences stored? What file format is often used for preference files?

10. What system preference enables the assistive technology features in OS X? What assistive technology features are available in OS X?

11. Where are Dashboard widgets installed when you double-click them? What process or processes are responsible for Dashboard widgets?

**Answers**

1. The system keeps applications from interfering with one another by segregating their memory usage using protected memory. Macs with 64-bit-capable processors allow processes to run in 64-bit mode, which allows them to individually access more than 4 GB of memory.

2. Using the Finder Get Info window you can force an application to open in 32-bit mode. This step is necessary for a 64-bit application to support older 32-bit plug-ins or application resources.

3. You can identify an application’s type with the Get Info or Inspector window in the Finder or with the System Information application.

4. You can use the System Information application to easily scan all the appropriate application locations and return a list of installed applications.

5. The Activity Monitor application is used to monitor open processes and applications.

6. General application troubleshooting steps include restarting the application, trying another known working document, trying another user account, checking log files, deleting cache files, replacing preference files, and replacing application resources.

7. The three ways to forcibly quit an application from the graphical interface are from the Force Quit Application dialog accessed from the Apple menu; from the Dock application shortcut menu accessed by Control-clicking or right-clicking the application’s icon; or from the /Applications/Utilities/Activity Monitor application.

8. The diagnostic reporting feature automatically springs into action any time an application crashes or hangs. This process creates a diagnostic report log that can be viewed immediately, reported to Apple via the Internet, or viewed later in the /Applications/Utilities/Console application.

9. Application preferences are almost always stored in the user’s Library folder in the ~/Library/Preferences folder. Most application preferences are property lists, which are XML-formatted files that use the “.plist” filename extension.
10. The OS X assistive technology features are available from the Accessibility preferences. This includes options to assist users who have difficulty seeing, hearing, using the keyboard, or interacting via keyboard, mouse, or trackpad.

11. When a user double-clicks Dashboard widgets, the system installs the widget to ~/Library/Widgets. The launchd process starts the Dashboard process on behalf of the currently logged-in user. All open widgets run inside the Dashboard process.

**Lesson 22 Review**

1. What do the terms “interface,” “protocol,” and “service” mean in relation to computer networks?

2. What is the purpose of Internet Protocol v4 (IPv4) addresses and subnet masks?

3. How does IPv4 addressing differ from IPv6 addressing?

4. How does the IP use the MAC address to send messages between computers on a local area network (LAN)?

5. How does the IP transfer messages between computers over a wide area network (WAN)?

6. How is the Domain Name Service (DNS) used to facilitate network naming?

7. What is used to identify a Wi-Fi network?

8. What Wi-Fi authentication protocols are supported by OS X?

9. How can an OS X system automatically connect to a Wi-Fi network?

10. Through what mechanism can a standard user configure Wi-Fi settings?

**Answers**

1. An interface is any channel through which network data can flow. Hardware network interfaces are defined by physical network connections, while virtual network interfaces are logical network connections that ride on top of hardware network connections. A protocol is a set of rules used to describe a specific type of network communication. Protocols are necessary for separate network devices to communicate properly. Finally, a network service (as it pertains to the Network preferences) is the collection of settings that define a network connection.

2. The Internet Protocol (IP) address identifies the location of a specific network device. IP addresses are the primary identification used by the Internet protocol suite TCP/IP for both local area and wide area networks. Subnet masks are used by network devices to identify their local network range and to determine if 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. An IPv6 address is a 128-bit number that is presented in eight groups of four-digit hexadecimal numbers separated by colons. This allows for a huge range of addresses, and as a result IPv6 addressing essentially includes subnet information.

4. If a network device needs to send data to another network device on the same LAN, it addresses the outgoing packets based on the destination device’s MAC address.

5. A network client uses the subnet mask to determine if the destination IP address is on the LAN. If the destination IP address is not on the LAN, it’s assumed 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, via a WAN connection, on 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 service is used to translate host names to IP addresses via forward lookups and translate IP addresses to host names via reverse lookups. DNS is architected as a hierarchy of worldwide domain servers. Local DNS servers provide name resolution and possibly host names for local clients. These local DNS servers connect to DNS servers higher in the DNS hierarchy to resolve both unknown host names and host local domain names.

7. A Service Set Identifier, or SSID, is used to identify a Wi-Fi network name and associated configuration.

8. OS X supports authenticated Wi-Fi via the following authentication protocols: WEP, WPA/WPA2 Personal, and WPA/WPA2 Enterprise, which includes support for 802.1X authentication.

9. A new OS X system can only automatically connect to Wi-Fi networks that have no standard authentication mechanism, otherwise known as an “open network.” However, a configured OS X system can automatically reconnect to authenticated Wi-Fi networks, provided that the appropriate information was saved to the Keychain system.

10. A standard user can connect to any non-WPA Enterprise Wi-Fi network via the Wi-Fi status menu. Because the system Keychain must be modified for WPA Enterprise connections, only an administrative user can establish these types of connections.
Lesson 23 Review

1. What is a network location? Who can access network locations?
2. What interfaces and protocols are supported by default in OS X?
3. What functionality does OS X support with the AppleTalk protocol?
4. How does network service order affect network connectivity?
5. In the Network preferences, how can you tell which interface is currently being used for network activities?
6. What is the easiest method on OS X to configure VPN settings?
7. How is 802.1X configured on OS X systems?

Answers

1. A network location is a saved state of the Network preferences that contains 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 via the Apple menu.

2. OS X supports the following network interfaces and protocols:
   - Wired 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 hardware network interface
   - Analog modem hardware network interface
   - Bluetooth wireless hardware network interface
   - USB connectivity via cellular network adapters
   - Virtual private network (VPN) virtual network interface via the Point-to-Point Tunneling Protocol (PPTP)
   - VPN virtual network interface via the Layer 2 Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec)
   - VPN virtual network interface via Cisco IPSec
   - Point-to-Point Protocol over Ethernet (PPPoE) virtual network interface
   - 6 to 4 virtual network interface
   - Virtual local area network (VLAN) virtual network interface via the IEEE 802.1Q standard
   - Link Aggregation virtual network interface via the IEEE 802.3ad standard
• Transmission Control Protocol/Internet Protocol (TCP/IP), also known as the Internet protocol suite
• Dynamic Host Configuration Protocol (DHCP)
• Domain Name Service (DNS) protocol
• Network Basic Input/Output System (NetBIOS) and Windows Internet Naming Service (WINS) protocols
• Authenticated Ethernet via the 802.1X protocol
• Point-to-Point Protocol (PPP)

3. OS X does not support AppleTalk.

4. The network service order list is used to determine the primary network service interface if there is more than one active service. All network traffic that isn’t better handled via local connection to an active network service interface is sent to the primary network service interface. Thus, in most cases all WAN traffic, Internet traffic, and DNS resolution is sent through the primary network service interface.

5. In the Network preferences, all network service interfaces with a green status indicator are being used for network activities. However, again, all network traffic that isn’t better handled via a local connection is sent to the primary network service interface. The primary network service interface is the topmost active interface in the listing.

6. The easiest method to configure VPN settings is use a configuration profile containing all the relevant VPN setup information.

7. On OS X there are two configuration methods for 802.1X. The first method is automatic configuration via the selection of a Wi-Fi network that requires WPA/WPA2 Enterprise authentication. The second method is “semi-automatic” configuration via an administrator-provided 802.1X configuration profile.

Lesson 24 Review

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

2. How do network devices acquire and use self-assigned TCP/IP addresses?

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

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. Four common issues that interrupt network services on Macs are:
   - Ethernet connectivity issues can cause the hardware network interface to become inactive or introduce excessive packet errors.
   - Wi-Fi connectivity issues caused by the selection of an improper Wi-Fi network or excessive wireless interference.
   - DHCP service issues prevent proper TCP/IP configuration.
   - DNS service issues prevent host name resolution.

2. If DHCP is specified as the configuration for a TCP/IP connection and no DHCP service is available, the device automatically selects a random IP address in the 169.254.xxx.xxx range. It checks the local network to ensure that no other network device is using the randomly generated IP address before it applies the IP address. In most cases, though, this addressing is not normal, and it's often indicative of a problem with DHCP services.

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

4. The Ping tab of Network Utility allows you to test basic connectivity to another network host by sending and then waiting for the return of a ping packet.

5. The Lookup tab of Network Utility allows you to test name resolution against the currently configured DNS server.

6. The Traceroute tab of Network Utility allows you to verify the connection hops between your Mac and a remote host.

**Lesson 25 Review**

1. What is the relationship between clients and servers as it relates to network service access?
2. What is the relationship between a network service and a network port?
3. What is the primary interface for configuring network service applications?
4. Which five network file services can you connect to from the Finder’s Connect to Server dialog?
5. How are items inside the Finder’s Network folder populated?
6. Which two methods can be used to automatically connect a network share?
7. What are three common troubleshooting techniques for issues involving failure to connect to network services?
8. How can you verify that a specific network service is available from a service provider?
9. What are some known issues that arise when connecting to network file services?

Answers

1. Client software is used to access network services provided by server software. The connection is established using a common network protocol known by both the client and server software. Thus, the client and server software can be from different sources.
2. Network services are established using a common network protocol. The protocol specifies which TCP or UDP port number is used for communications.
3. The Mail, Contacts, & Calendars preference is the primary interface in OS X for configuring built-in network applications.
4. From the Finder’s Connect to Server dialog, you can connect to Apple File Protocol (AFP), Server Message Blocks/Common Internet File System (SMB/CIFS), Network File System (NFS), Web-based Distributed Authoring and Versioning (WebDAV), and File Transfer Protocol (FTP) network file services.
5. The Finder populates the Network folder using information provided by the dynamic network services discovery protocols. Computers providing services appear as resources inside the Network folder, while service discovery zones or workgroups appear as folders. Any currently connected servers also appear in the Network folder.
6. To automatically connect a file share when the user logs into the system, drag the share from the Finder to the user’s login items in the Users & Groups preferences. Alternatively, 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.
7. Review the Network preferences, review the Network Utility statistics, and attempt to connect to different network services.
8. To verify 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 the specific service port(s) are open. You should always limit the port scan to the specific ports required for the network service you are testing.
9. Files with metadata may cause problems for NFS or WebDAV network file systems. Also, avoid AFP 2 services provided by Windows file servers.

**Lesson 26 Review**

1. How does OS X use dynamic network service discovery protocols to access network services?
2. Which two dynamic network service discovery protocols are supported by OS X?
3. Which sharing services can OS X provide?
4. What is the security risk of enabling client sharing services?
5. Which application can provide on-demand screen sharing even when the Screen Sharing service isn’t enabled?
6. What is AirDrop, and how do you know if a specific Mac supports it?
7. How does the OS X built-in firewall work?
8. Which optional firewall settings are available?

**Answers**

1. Devices providing a network service advertise their availability via a dynamic network service discovery protocol. Clients looking for services request and receive this information to provide the user with a list of available network service choices.
2. OS X supports Bonjour and Server Message Block (SMB), including support for legacy Network Basic Input/Output and Windows Internet Naming Service (NetBIOS and WINS) dynamic network service discovery protocols.
3. The OS X sharing services include DVD or CD sharing, Screen Sharing, File Sharing, Printer Sharing, Scanner Sharing, Remote Login, Remote Management (ARD), Apple Events, Internet Sharing, and Bluetooth Sharing.
4. If a client sharing service is compromised, an unauthorized user can control your Mac and execute unwanted applications or processes.
5. The Messages application allows for on-demand screen sharing that can be used even when the system screen sharing service isn’t enabled.
6. AirDrop provides a quick and easy method to share files locally via Wi-Fi. AirDrop creates a secure peer-to-peer network between local Macs. You can verify that a Mac supports AirDrop from the Finder Go menu.
7. The OS X built-in firewall inspects each incoming network connection to determine if it’s allowed. Connections are allowed or denied on a per-application basis.

8. The optional firewall settings let you control whether signed applications are automatically allowed through the firewall, control the list of allowed (or denied) applications, and enable stealth mode (which means your Mac will not respond to any unsolicited connections).

**Lesson 27 Review**

1. What are the four primary peripheral bus technologies supported by Macs running OS X?

2. Which action must take place in order for a Mac to communicate with a Bluetooth peripheral? Where can this be configured?

3. What is a device driver? Which three primary types of device drivers are there?

4. How does OS X support third-party devices without needing third-party device drivers?

5. What can you infer about a connected peripheral if it does not appear in the System Information application?

**Answers**

1. The four primary peripheral bus technologies supported by OS X are: Universal Serial Bus (USB), FireWire, Thunderbolt, and Bluetooth wireless.

2. Bluetooth devices must be paired to each other for communication to occur. The Bluetooth Setup Assistant is responsible for pairing your Mac with Bluetooth peripherals. You can open the Bluetooth Setup Assistant from the Bluetooth status menu or the Bluetooth preferences.

3. A device driver is software specially designed to facilitate the communication between OS X and a peripheral. Device drivers can be kernel extensions, framework plug-ins, or standalone applications.

4. OS X uses built-in generic drivers based on each device class. For example, there are generic drivers for scanners and printers that can be used in lieu of official third-party drivers.

5. If a connected peripheral does not appear in System Information, the issue is likely to be hardware related. Troubleshoot accordingly.
Lesson 28 Review

1. What does CUPS do?
2. What are PPD files responsible for?
3. What is the best source for acquiring printer drivers for OS X?
4. Under what circumstances can a standard (non-administrative) 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 issues, what is a potential quick fix?

Answers

1. Common UNIX Printing System (CUPS) manages all printing for OS X, including both local and shared printing.
2. PostScript Printer Description (PPD) files are printer driver files that instruct the CUPS system on how to communicate with specific printer models.
3. The Apple print drivers are the best source for configuring OS X printers. One method is to let the software update system automatically download and install the appropriate printer drivers. Alternately, you can manually download and install printer drivers from the Apple support website.
4. Assuming the default settings for OS X, a standard user can only configure directly attached or local network printers from the Print dialog. Also, the appropriate drivers must be installed prior to the standard user configuring the printer.
5. You can enable printer sharing from the Print & Scan or Sharing preferences. Note that Windows clients may need additional drivers to access the Mac computer’s shared printers via the IPP protocol.
6. In OS X Mountain Lion, from the Print & Scan preferences, to select a new printer driver for a configured printer you must delete and then re-add a printer.
7. If all printers appear to be having issues a quick fix is to reset the entire printing system by using secondary (or Control) click in the printer list and then choosing “Reset printing system.”
Lesson 29 Review

1. What are the primary system initialization stages in OS X? What are the visual and/or audible cues of these items?
2. What does the firmware do? What is the POST?
3. What role does the system launchd process serve during system startup?
4. Which items are automatically started by the system launchd during the system initialization process?
5. What are the primary user session stages in OS X? What are the visual and/or audible cues of these items?
6. What is 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 system shutdown?

Answers

1. Each primary stage of system initialization can be indicated by the following: firmware, startup chime or bright flash of the power-on light followed by a light gray screen on the primary display; booter, a dark gray Apple logo on the primary display; kernel, a small dark gray spinning gear or spinning earth icon below the Apple logo; and system launchd, a white screen on all displays followed by the login screen.
2. The firmware initializes the Mac computer’s hardware and locates the booter file on a system volume. The Power-On Self-Test (POST) checks for basic hardware functionality when your Mac powers on.
3. The system launchd process is ultimately responsible for starting every system process. It also manages system initialization and starts the loginwindow process.
4. During system initialization the system launchd process automatically starts /System/Library/LaunchDaemons, /Library/LaunchDaemons, /Library/StartupItems (via SystemStarter), and the /etc/rc.local UNIX script if it exists.
5. Each primary stage of the user session can be indicated by the following: the loginwindow process displays the login screen; the user launchd process loads applications like the Finder after user authentication; and the user environment is active any time the user is logged into the system.
6. Launch daemons and startup items open during system initialization by the system `launchd` process on behalf of the root user. Launch agents and login items open during the initialization of the user environment by the user’s specific `launchd` process.

7. Safe Sleep is a feature of all OS X compatible portable Macs that saves the system’s state to permanent storage in cases where the Mac’s battery drains completely. Power Nap is a feature of Mac systems introduced after mid 2011 that use all flash storage. Power Nap allows the Mac to automatically wake in a low-power mode so the system can perform a variety of application and system updates.

8. During user logout the user’s `loginwindow` process does the following: requests that all user applications quit; automatically quits any user background processes; runs any logout scripts; records the logout to the main system.log file; resets device permissions and preferences to their defaults; and quits the user’s `loginwindow` and `launchd` processes.

9. At system shutdown the `loginwindow` process logs all users out and then tells the kernel to quit all remaining system processes. Once the kernel quits all system processes, the Mac shuts down.

**Lesson 30 Review**

1. Which keyboard shortcut is used to Safe Boot OS X?
2. Which keyboard shortcut can be used to temporarily choose another startup disk?
3. Which changes are made when OS X Safe Boots?
4. Which items are not loaded when OS X Safe Boots?
5. How do you further resolve an issue that disappears when the Mac successfully safe-boots?

**Answers**

1. A Safe Boot is initiated by holding down the Shift key during system startup.
2. Holding the Option key at startup opens Startup Manager, which allows you to temporarily choose another startup disk.
3. When OS X Safe Boots it performs the following permanent actions: attempting to repair the system volume structure, deleting system KEXT caches, and deleting font caches.
4. When OS X Safe Boots, it does not load third-party 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.

5. If an issue disappears when the Mac successfully Safe Boots, you must find and remove the third-party startup resource that caused the issue. The best way to isolate the problematic item is to start up the Mac in Verbose mode and then observe where the startup process fails. Verbose mode is initiated by holding down Command-V during system startup.