OS X Support Essentials 10.9
Exam Preparation Guide

Updated March 2014
Contents

About This Guide ..............................................................................................................3
Becoming an Apple Certified Support Professional ..................................................3
Exam Details .....................................................................................................................4
Recommended Exam Preparation ..............................................................................5
Part One: Installation and Configuration ..................................................................6
Part Two: User Accounts ...............................................................................................12
Part Three: File Systems ...............................................................................................18
Part Four: Data Management .......................................................................................24
Part Five: Applications and Processes .......................................................................30
Part Six: Network Configuration ..................................................................................36
Part Seven: Network Services .......................................................................................43
Part Eight: System Management ..................................................................................47
About This Guide

This guide provides all the information you need to prepare to earn the Apple Certified Support Professional (ACSP) certification. From this guide you can:

- Learn about Apple Certification
- Find out how to take the exam
- Locate resources to help you prepare for the exam
- Review the range of objectives that the exam may cover
- Get a feel for the type of questions that appear on the exam

Becoming an Apple Certified Support Professional

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

Apple offers four OS X certifications:

- Apple Certified Associate - Mac Integration
- Apple Certified Associate - Mac Management
- Apple Certified Support Professional (ACSP)
- Apple Certified Technical Coordinator (ACTC)

Apple Certified Support Professional (ACSP) certification verifies an understanding of OS X core functionality and an ability to configure key services, perform basic troubleshooting, and support multiple users with essential OS X capabilities. ACSP certification is designed for the help desk professional, technical coordinator, or power user who supports OS X users, manages networks, or provides technical support for the Mac.

Students earn ACSP certification by passing the OS X Support Essentials 10.9 Exam.

For more information on all OS X certifications, go to http://training.apple.com/certification/osx10.

What are the benefits of ACSP Certification?

Besides differentiating you as a skilled user and support professional for OS X Mavericks, ACSP certification allows you to leverage the power of the Apple brand. When you pass the certification exam, you receive an email detailing 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 to make it easy for you to share your certification news with your networks on these sites.
You also receive a login for the Apple Certification Records System, where you can:

- Update your profile information and opt in to display your Apple Certification on the Apple Certified Professionals Registry
- Review your certification progress
- Download your certification logo to use on business cards, résumés, websites, and more
- Provide access to employers to verify your certifications

**Exam Details**


The OS X Support Essentials 10.9 Exam is a computer-based test offered at Apple Authorized Training Centers (AATCs). To find the closest AATC, go to [training.apple.com/locations](http://training.apple.com/locations).

Many AATCs schedule certification exam sessions at [training.apple.com/schedule](http://training.apple.com/schedule). If you don’t see a session scheduled at your nearest AATC, contact the AATC to find out whether a session can be scheduled. **Note: All AATCs offer all OS X and pro apps exams, even if they don’t offer the corresponding course.**

The OS X Support Essentials 10.9 Exam details are as follows:

- **Exam number:** 9L0-415.
- **Approximately 80 technical questions.**
- **Five unscored demographic questions.**
- The exam uses a random pool of multiple-choice, fill-in-the-blank, true/false, and interactive-media questions.
- **Passing score:** 75 percent (scores are *not* rounded).
- Details on exam scoring are at [training.apple.com/certification/faq](http://training.apple.com/certification/faq).
- **Exam duration:** Two hours.
- Some exams are also available in other languages; for details, go to [training.apple.com/certification/localized](http://training.apple.com/certification/localized).

The exam timer doesn’t start until you view the first technical question. You may not access any resources or references during the exam.

If you have additional questions about exams, please go to [training.apple.com/certification/faq](http://training.apple.com/certification/faq) for more information.
Recommended Exam Preparation

The following exam preparation strategies are recommended:

- Gain experience with OS X.
- Review the objectives and questions in this guide.

Gain experience with OS X

Nothing can substitute for time spent learning the technology. After you read the book and/or take the class, spend time increasing your familiarity with OS X on your own to ensure your success on the certification exam.

Learn from experts

Apple Authorized Training Centers (AATCs) offer classes where you can learn hands on with the technology and benefit from the expertise of Apple Certified Trainers and your peers. Go to the Apple Training and Certification website to find course offerings at nearby AATCs.

Study the Apple Pro Training Series book

Apple Pro Training Series books are the basis for the related Apple certification exams. The book for this exam is Apple Pro Training Series OS X Support Essentials 10.9. You can purchase the book at peachpit.com (click here for a 30 percent discount code). Creative Edge, an on-demand digital library, offers subscription access to the Apple Training and Apple Pro Training Series, as well as thousands of other reference videos and books. If you use an iPad, you can get an electronic version on the iBooks Store. Some books are also available in other languages. Click here for details.

Review the objectives and questions

Even if you’re self-taught, or have taken courses that don’t use the Apple Pro Training Series curriculum, you can still prepare for the certification exam by making sure that you can complete all the tasks and answer all the review questions in the following sections.

The exam objectives describe the knowledge domains assessed by the exam. The review questions summarize what you should have learned in each lesson. Please note that although this guide divides the objectives into lessons or knowledge areas, questions are presented randomly during the exam.

The number of test questions drawn from each knowledge area is indicated for each of the following lessons.
Part One: Installation and Configuration

After completing Part One, “Installation and Configuration,” in OS X Support Essentials 10.9, you should be able to complete the following tasks. Eleven items from Part One are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Describe the process for creating an external Mavericks Recovery volume.
- State the methods by which the Mavericks installer may be obtained.
- State the minimum hardware and software requirements to install OS X Mavericks.
- State the current minimum hardware and software requirements.
- Given a Mac with OS X installed, verify that the computer meets the minimum hardware requirements to install the latest OS X software.
- List four critical steps that should be taken before installing OS X.
- State the types and sources of data that Migration Assistant can migrate data from.
- Given a Mac with Internet access, identify the latest version of firmware available for the computer.
- Navigate to the Support or Downloads pages on the Apple website to find the latest compatible firmware update.
- Describe the process for reinstalling OS X using the Mavericks Recovery volume.
- Describe how formatting a Mac computer’s hard disk into a single partition can simplify the process of preparing to install OS X.
- Describe how formatting a Mac computer’s hard disk into multiple partitions can simplify the process of configuring and using the Mac.
- Describe how maintenance of multiple operating systems can be simplified by installation on a multiple-partition drive.
- Describe how keeping operating system data and user data separate can be simplified by installation on a multiple-partition drive.
- Describe the OS X installation process, including decisions made in response to Installer interface options.
- List the utilities available to the user when a Mac is booted from the OS X recovery volume.
- Configure a Mac with OS X for use on a local area network with Internet access.
- State where in the GUI interface you configure a Mac computer’s network settings.
- Describe how configuration profiles are used to manage settings on an OS X computer running Mavericks.
- Describe how Setup Assistant is used to configure settings on an OS X computer running Mavericks.
• Compare and contrast the five categories of preferences in System Preferences: Personal, Hardware, Internet & Wireless, System, and Other.

• Describe how software and security updates are made available to client computers via the Software Update preference pane in System Preferences, and the Software Update and App Store items in the Apple menu.

• Given a Mac with OS X installed, identify any updates that have been installed.

• Define the system terms “version number,” “build number,” and “serial number” as they pertain to an installation of OS X.

• Given a Mac with OS X installed, identify the system version number, build number, and serial number.

Lesson One review questions
Lesson One doesn't include any review questions.

Lesson Two review questions
After completing Lesson Two, you should be able to answer the following questions.
1. What are the minimum hardware requirements for upgrading a system with OS X Mavericks?
2. What four preparation steps must you take before upgrading a system with OS X Mavericks?
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 Mavericks installer?
6. What options can you select from during the OS X Mavericks installation?

Answers
1. The minimum requirements for upgrading OS X Mavericks 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
   • Compatible Mac model (as listed on www.apple.com/osx/specs/)
2. Four steps you should take before upgrading a system to OS X Mavericks are:
   • Install Apple software and firmware updates
   • Verify application compatibility
   • Back up important files and folders
   • 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 Mavericks installer can be downloaded from the Mac App Store for free.

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

Lesson Three review questions
After completing Lesson Three, you should be able to answer the following questions.

1. What process is used to guide a user through the initial configuration of OS X Mavericks?
2. What key features do you gain by setting up iCloud?
3. Aside from initial OS X configuration, where can you manage iCloud settings?
4. What three primary sources can Migration Assistant pull from?
5. What are the five System Preference categories?
6. How do the four default System Preferences categories differ?
7. What’s a profile? How are profiles managed?
8. Where can you locate the system version number, build number, and serial number? What’s the significance of these numbers?
Answers

1. The Setup Assistant process guides a user through initial configuration of OS X Mavericks.

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

3. After initial OS X setup, iCloud settings can be managed from iCloud or Internet Accounts preferences.

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

5. System Preferences is divided into five categories, from top to bottom; Personal, Hardware, Internet & Wireless, System, and Other.

6. 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.

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

8. 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 Four review questions

After completing Lesson Four, you should be able to answer the following questions.

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 to reinstall OS X Mavericks?

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


2. The local hidden OS X Recovery HD doesn’t include the OS X installation assets. So reinstalling OS X Mavericks from here requires high-speed Internet access and the ability to verify access to the installation assets. Upgraded Mac systems are verified by entering the Apple ID used to purchase OS X Mavericks. Verification is automatic for Mac systems that included OS X Mavericks when purchased new.

3. The OS X Recovery Disk Assistant can create a small OS X Recovery disk that lacks the OS X installation assets. An OS X Installation disk, which includes the full OS X installation assets, can be created by using the createinstallmedia command line tool found inside the Install OS X Mavericks application.

Lesson Five review questions

After completing Lesson Five, you should be able to answer the following questions.

1. Which application can you open to initiate Apple software updates?
2. By default, what items are always installed via automatic software updates?
3. How can you prevent a user from installing software updates?
4. Which applications are used to manually acquire and install OS X software updates?
5. What’s the best way to find which installations have taken place on the system?

Answers

1. All Apple software updates are handled via the Mac App Store.
2. By default, system files and security updates are automatically installed when available.
3. You can prevent automatic updates for all users by disabling the options in App Store preferences. You can further restrict a user’s ability to use the Mac App Store by configuring Parental Controls for the user’s account.
4. 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.
5. The Installations section of System Information will show the history of all software installed via the Mac App Store or the OS X Installer.
Part Two: User Accounts

After completing Part Two, “User Accounts,” in OS X Support Essentials 10.9, you should be able to complete the following tasks. Eleven items from Part Two are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

• Given a Mac with OS X installed, create and manage user accounts.
• Describe the key features and benefits of iCloud supported on a Mac running OS X Mavericks.
• Describe the process for deleting a user account on an OS X computer running Mavericks and the result of deleting the account.
• Describe the process for restoring a user account on an OS X computer running Mavericks.
• List the five types of user accounts in OS X.
• Compare and contrast the five types of users.
• Identify the three attributes of user accounts in OS X.
• Describe a security risk related to enabling the Guest account in OS X.
• Describe a security risk related to enabling the root user account in OS X.
• Describe a security risk related to enabling the sharing user account in OS X.
• Describe a security risk related to using an administrator account as the primary user account in OS X.
• Describe an advantage related to using an administrator account as the primary user account in OS X.
• List the default folders in a user home folder.
• Compare and contrast the functions of each of the default folders in a user's home folder in OS X.
• List the resources that an administrator can limit in the Parental Controls preference pane in System Preferences.
• Describe three errors that can occur when fast user switching is enabled and two users access the same file or peripheral in OS X.
• Describe messages indicating that the file, peripheral, or application is busy.
• Describe errors that can occur when fast user switching is enabled and two users access the same application simultaneously.
• Describe how some applications can't be opened at the same time by more than one user.
• Describe a security risk that can result when fast user switching is enabled and other local users switch to their accounts.
• Describe how users who fast-switch to their accounts can access volumes mounted by other logged-in users.
• Given a Mac with OS X installed, secure the user environment.
• Describe how to enable and disable the firmware password.
• Describe the functions and features of the keychains in OS X.
• Describe how to reset a user account password using an Apple ID.
• Describe the privacy controls available for a user account.
• Describe the security features offered by iCloud for Mac computers running OS X Mavericks.
• Compare and contrast the methods for changing and resetting passwords.
• Compare and contrast how each of these passwords function in OS X: login, firmware, resource, keychain, and Apple ID.
• Compare and contrast the roles of keychains, keychain items, and keychain first aid.
• Describe how resetting a user account password can cause the keychain and user account password to get out of sync.
• Describe the requirements necessary for FileVault 2 to unlock accounts that were initially encrypted with Legacy FileVault.
• Describe how the Firmware password feature prevents users from changing passwords for user accounts other than their own.

Lesson Six review questions
After completing Lesson Six, you should be able to answer the following questions.

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 doesn’t require a password; sharing-only users can access only shared files; and the root user has unlimited access to any file or folder in the system.
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 further limit a user account. Examples include enforcing a simple Finder, limiting applications and widgets, limiting Mac App Store content, 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 Seven review questions

After completing Lesson Seven, you should be able to answer the following questions.

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 Users & Groups preferences 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 after you create the new user in Users & Groups preferences with the same account name, the system will prompt you to associate the new account with the restored home folder.

Lesson Eight review questions

After completing Lesson Eight, you should be able to answer the following questions.

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 is 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 won’t change any keychain passwords. Therefore, the user’s keychains won’t 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 can’t be reset by the new master password.
6. The Privacy pane of Security & Privacy preferences can be used to allow or disallow applications’ access to Location Services, Contacts, Calendars, Reminders, social network services, and Accessibility application access.
7. iCloud Find My Mac allows you to remotely locate a lost Mac system. You enable this feature in iCloud preferences. To locate a lost Mac system, you can use the iCloud website or the Find My iPhone app on an 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 Nine review questions
After completing Lesson Nine, you should be able to answer the following questions.

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?
5. When and why would you set up an iCloud Security Code?
6. What's required to set up the iCloud Keychain service on multiple Apple devices?

Answers

1. Keychains are used to store secrets such as resource passwords, digital certificates, and encryption keys. The keychain system can also securely store Safari AutoFill information, Internet Account settings, and secure text notes.

2. The keychain system manages encrypted files that are used to securely save your items. By default, every user has login and Local Items keychains that use 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 login keychain saved at /Users/<username>/Library/Keychain/login.keychain and a Local Items/iCloud keychain saved in the /Users/<username>/Library/Keychains/<UUID> 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.

5. An iCloud Security Code can be set up the first time you enable the iCloud Keychain service for a specific Apple ID. The iCloud Security Code can be used to set up other devices for the iCloud Keychain service and can be used to regain access to the iCloud keychain should you lose all your Apple devices.
6. Additional Apple devices must be authorized to use the iCloud Keychain service using a combination of the Apple ID password and another method. One method involves using an iCloud Security Code; the other method is to authorize access from another Apple device that has already been configured for the iCloud Keychain service.
Part Three: File Systems

After completing Part Three, “File Systems,” in *OS X Support Essentials 10.9*, you should be able to complete the following tasks. Eleven items from Part Three are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Describe the implications and process for converting Legacy FileVault data to FileVault 2.
- State the requirements for FileVault 2.
- Describe how to securely erase the remaining space on a drive connected to a Mac running OS X Mavericks.
- Describe how to force eject an item that’s in use.
- Describe the tools and methods used to reset home folder permissions.
- Describe the tools and methods used to enable FileVault 2 on a volume connected to a Mac running OS X Mavericks.
- Describe the tools and methods used to decrypt a FileVault 2–encrypted volume using a recovery key.
- Describe the tools and methods used to gather information about the format, partition scheme, bus type, and available space on local hard disks and volumes.
- Use Disk Utility and System Information.
- Differentiate between hard disks, partitions, and volumes.
- Compare and contrast GUID, APM, and MBR partition map schemes.
- Compare and contrast the volume formats supported by OS X:
  - Mac OS Extended
  - Mac OS Extended Journaled
  - Journaled
  - Mac OS Extended Journaled, Case-Sensitive
  - UFS
  - FAT32
  - NTFS
  - ExFAT
  - Mac OS Extended (Journaled, Encrypted).
- Describe how file system journaling works in OS X.
- Describe how FileVault 2 secures user data.
- Describe the Verify and Repair features of Disk Utility.
- Compare and contrast the erase options available in Disk Utility, (including single-pass, 3-pass, and 7-pass erases).
- Describe the function of the Secure Empty Trash feature in the Finder.
• Describe how power failures and force ejecting a disk can corrupt a volume.
• Identify three ways to unmount a disk from the Finder in OS X.
• Describe Target Disk Mode.
• Given a Mac with OS X installed, manage file ownership and permissions.
• Describe how the Get Info window in the Finder can be used to manage permissions for files and folders.
• Describe how Disk Utility can be used to repair permissions for files and folders.
• Describe the function of each of the permission settings and ACL settings on OS X files and folder.
• Given a Mac with OS X installed, identify the owner and group for any file.
• Use the Get Info command in the Finder.
• Identify the owner and group permission settings for users' home folders in OS X.
• Describe why the root of any user's home folder in OS X is accessible to other users.
• Describe the permissions settings on the Shared folder in OS X that allow it to act as a shared storage location for local user accounts.
• Describe what it means to “ignore volume ownership,” including when it's useful to do so, and one potential risk when ignoring ownership.
• Describe how anyone can access any file on the drive while ownership is ignored.
• Describe how the organization of the OS X file system allows multiple users to safely share local files and folders.
• Define the term “sticky bit” as it applies to the OS X file system.

Lesson Ten review questions
After completing Lesson Ten, you should be able to answer the following questions.

1. How are disks, partitions, and volumes different from one another?
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? How are they all different?
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 losing its contents?

9. What four methods can be used to eject a volume or disk from the Finder?

10. What's 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 Mac computers, and Apple Partition Map is the default partition scheme on PowerPC-based Mac computers.

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
   - 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 losing 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:
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 eject and choose Eject from the File menu.

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 Eleven review questions

After completing Lesson Eleven, you should be able to answer the following questions.

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 before FileVault 2 can be enabled.

3. Any user that’s 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 Security & Privacy preferences 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 Twelve review questions

After completing Lesson Twelve, you should be able to answer the following questions.

1. How do you identify the ownership and permissions of a file or folder in the Finder?
2. How do ACLs differ from standard UNIX file system permissions?
3. What's 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's 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 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 don't 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's a potential security risk because it will allow any
local user account to have full access to the volume, even if that user didn’t originally mount the volume.

Lesson Thirteen review questions
After completing Lesson Thirteen, you should be able to answer the following questions.

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’s 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?

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 disks through the FireWire ports. Target disk mode can be engaged from 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.
Part Four: Data Management

Upon completion of Part Four, “Data Management,” in *OS X Support Essentials 10.9*, you should be able to complete the following tasks. Twelve items from Part Four are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Given a Mac with OS X installed, manage user and system files.
- Compare and contrast the features and functions of aliases and links as implemented in OS X.
- Describe the tools and methods used to create aliases and links.
- Describe the structure and purpose of the AppleDouble metadata format.
- Describe the tools and methods used to navigate to and view the contents of hidden folders in the Finder.
- Describe the tools and methods used to install fonts.
- List the four default top-level folders visible in the Finder: Applications, Library, System, and Users.
- Describe the types and function of metadata as it applies to the file system.
- Compare and contrast the System, Local, User, and network domains, including what resources are stored in each, and the order in which OS X searches for resources in the file system.
- Describe OS X extended attributes, and give one example of information the system keeps as an extended attribute.
- Compare and contrast these file types: extensions, frameworks, fonts, preferences, startup items, and logs.
- Compare and contrast file system packages and bundles, and their purposes.
- Identify where each of these file types are located in the file system: extensions, frameworks, fonts, preferences, startup items, and logs.
- Describe how Spotlight metadata is used in OS X.
- Describe how and why the Finder hides certain folders by default.
- Identify potential privacy and security issues with Spotlight.
- Describe where metadata indexes and plug-ins are stored in the OS X file system.
- Given a Mac with OS X installed, archive files.
- Describe the tools and methods used to manage a zip archive of selected items in the Finder.
- Compare and contrast disk images created with Disk Utility and zip archives created by the Finder in OS X.
- Describe the options available when creating a new blank image using Disk Utility in OS X.
- Given a Mac with OS X installed, configure and manage Time Machine.
• Describe how encryption is utilized in a Time Machine backup.
• Describe the tools and methods used to configure Time Machine to backup and restore data from specific volumes to specific destinations.
• Describe how Time Machine functions.
• Identify the files that are always omitted from Time Machine backups.
• Describe issues with backing up large database files that are frequently updated.
• List issues such as space limitations that interfere with backups.
• Describe the archive format used by Time Machine.
• Describe why a specific archived file may not be available due to backup or retention schedule parameters.

Lesson Fourteen review questions

After completing Lesson Fourteen, you should be able to answer the following questions.

1. Why does the Finder hide certain folders at the root of the system volume?
2. What two methods are used to hide items from the Finder?
3. What does 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 need access to these UNIX items, they can access them from Terminal.
2. The Finder doesn’t show items with periods at the beginning of their filenames or items with the hidden file flag enabled. Both methods for hiding items can only be managed from the command line interface.
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 if it’s renamed or moved within the same volume. Whereas any change to an original item breaks a symbolic link.
Lesson Fifteen review questions

After completing Lesson Fifteen, you should be able to answer the following questions.

1. What are the four default top-level folders visible in the Finder?

2. What are six common system resources? What purpose does each resource serve? Where are they located in the file hierarchy?

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 will you find in this folder?

5. What happens when a user double-clicks a font file?

6. 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
   - 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 needed at system startup, or at user login
   - 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

• System, containing applications and system resources required to provide basic system functionality

4. The ~/Library/Containers folder contains resources for sandboxed applications. The system creates and maintains a separate container folder for each sandboxed application the user opens. A sandboxed application is more secure because it can only access items inside its container.

5. 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.

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

Lesson Sixteen review questions

After completing Lesson Sixteen, you should be able to answer the following questions.

1. What's 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. 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? How about the Spotlight plug-ins?
6. What are some privacy and security concerns with the Spotlight service?
7. How do you resolve an issue where a Spotlight search doesn't find 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. File system tags are a type of metadata that allow you to quickly assign keywords, or “tags” to any item. The user can customize the tag names and colors.
4. The Spotlight search service creates index databases of file system metadata so that it can perform normally time-intensive searches nearly 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 his encrypted home folder. And 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.

6. 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.

7. 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 Seventeen review questions

After completing Lesson Seventeen, you should be able to answer the following questions.

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 contents of the zip archive 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 they offer greater flexibility. Primarily, disk images can be easily modified.
and converted. However, OS X style disk images aren’t compatible with third-party operating systems.

Lesson Eighteen review questions
After completing Lesson Eighteen, you should be able to answer the following questions.

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 haven’t 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 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 won’t 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
   - Restoring a user account via Migration Assistant
   - Restoring an entire system via OS X Recovery
   - Manually restoring items via the Finder
Part Five: Applications and Processes

After completing Part Five, “Applications and Processes,” in OS X Support Essentials 10.9, you should be able to complete the following tasks. Twelve items from Part Five are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Given a Mac with OS X installed, manage and support applications.
- Describe the methods and mechanisms by which files can be locked and unlocked.
- Describe the features and functions of Quick Look.
- State the location of Quick Look plug-ins.
- State the file types supported by Quick Look in a default installation of OS X.
- State which applications included with OS X use Quick Look.
- Describe the key features of the App Store application.
- Describe the key requirements for using the App Store application to purchase and install applications.
- Describe the process for signing in and out of the App Store using a valid Apple ID.
- Verify the currently active Apple ID that's being used with the App Store.
- Describe the features, purpose, and operation of the Auto Save function.
- Describe the features, purpose, and operation of the Versions function.
- Describe the requirements and process for running Java applications on OS X.
- Describe the purpose and benefit of application sandboxing as implemented in OS X.
- Compare and contrast 32- and 64-bit modes of operations for OS X applications.
- Compare and contrast the traditional installation of applications on OS X via drag and drop and installation packages.
- Describe the tools and methods for updating applications that have been installed using traditional drag and drop or installation packages.
- Compare and contrast the tools and methods for removing applications in OS X via Launchpad, Trash, and uninstallers.
- Describe the tools and methods used for managing documents between iCloud and a compatible application.
- Describe the dictation feature of OS X Mavericks.
- Identify the languages and commands supported by the dictation feature.
- Define protected memory.
• Describe the application environments supported by OS X.
• Define 64-bit memory addressing.
• Given a Mac with OS X installed, identify processes and applications that are using a significant percentage of RAM or processor time.
• Use Activity Monitor.
• Given a Mac with OS X installed, list installed applications.
• Use System Information.
• Identify three ways to force quit an application.
• Describe how the Finder in OS X identifies which application should be used to open a file.
• Describe where application preferences are stored.
• Describe the format of preference files.
• Identify the preference pane that enables Accessibility features in the Finder and other applications.
• Describe the tools and methods for using the VoiceOver feature.
• Describe the Accessibility features and functions in OS X.
• Describe how to troubleshoot application environment issues in OS X.
• Given a Mac with OS X installed, install and remove applications.
• Describe the function, purpose, and benefits of the Resume feature in OS X Mavericks as it relates to Auto Save and Versions.
• Describe the tools and methods that are used to control the Resume feature in OS X Mavericks.
• Describe the diagnostic reporting and log features supported in the Console application included with OS X.
• Describe the function, purpose, and benefits of the Gatekeeper feature as it relates to installing applications.
• Compare and contrast the three security options supported by Gatekeeper.
• Describe how Dashboard widgets work.
• Describe the security implications of installing Dashboard widgets.

Lesson Nineteen review questions
After completing Lesson Nineteen, you should be able to answer the following questions.

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 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, and an Internet connection.

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
   - UNIX applications, which are primarily accessed via Terminal
   - Java applications, which work as cross-platform applications
   - X Window System applications, which run inside the popular UNIX windowing environment

   OS X doesn't 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're otherwise completely cut off from the rest of the system, so they can't cause 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:
   - Open Launchpad, hold down the Option key, and click the “X” button
   - In the Finder, drag the primary application to the Trash and then empty the Trash
   - Use a custom-built uninstaller package

Lesson Twenty review questions
After completing Lesson Twenty, you should be able to answer the following questions.

1. In OS X, what’s 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’s 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 Auto Save and 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’re capable of opening.

2. Quick Look is engaged by simply pressing the Space bar when a document is selected. Applications that support Quick Look include the 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 allows compatible OS X applications to automatically save changes to users’ documents. A user just
saves a document once, then 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 don’t 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 don’t appear anywhere in the Finder that a user would normally look.

8. You can deselect the option to “Reopen windows when logging back in” from the logout verification dialog. You can deselect the option to “Close windows when quitting an application” from General preferences. Also from General preferences, you can select the option to “Ask to keep changes when closing documents,” which turns off the Auto Save feature.

Lesson Twenty-one review questions

After completing Lesson Twenty-one, you should be able to answer the following questions.

1. What’s protected memory? What’s 64-bit memory addressing?

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

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

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

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

6. What three ways can you forcibly quit an application from the graphical interface?

7. What does the diagnostic reporting feature do?

8. Where are application preferences stored?

9. What file format is often used for preference files? How can you view the content of this type of file?

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

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. Mac computers 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 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 use the System Information application to easily scan all the appropriate application locations and return a list of installed applications.

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

5. 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.

6. 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.

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

8. Application preferences are almost always stored in the user’s Library folder in the ~/Library/Preferences folder. Newer sandboxed applications 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 application.

9. Most application preferences are property lists, which are XML-formatted files that use the “.plist” filename extension. The content of these files can be viewed using Quick Look, and edited using the Xcode development application found on the Mac App Store.

10. The OS X assistive technology features include options to assist users who have difficulty seeing, hearing, using the keyboard, or interacting via keyboard, mouse, or trackpad. These features are available from Accessibility preferences.
11. When a user double-clicks a Dashboard widget, 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.

Part Six: Network Configuration

After completing Part Six, “Network Configuration,” in OS X Support Essentials 10.9, you should be able to complete the following tasks. Seven items from Part Six are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Discuss TCP/IP networking concepts.
- Discuss the purpose and format of Internet Protocol (IP) addresses and subnet masks.
- Describe how the Internet Protocol uses a MAC address to send messages between computers over a local area network (LAN).
- Describe how the IP transfers messages between computers over a wide area network (WAN), including how IP addresses, subnet masks, and routers work.
- Describe how domain name service (DNS) is used to associate computer host names with IP addresses on a network.
- Define the terms “service,” “interface,” and “protocol.”
- Given an IPv4 address, IPv6 address, and MAC address, identify each.
- Given a Mac with OS X installed, configure and manage a network interface.
- Describe how computers are assigned IP addresses from a DHCP server.
- Describe how OS X connects to Wi-Fi networks upon startup or wake.
- Describe the criteria by which a Mac with OS X installed and functional Wi-Fi hardware auto-connects to a Wi-Fi network.
- Describe the types of secure Wi-Fi networks that a Mac with OS X installed and functional Wi-Fi hardware can connect to.
- Describe how OS X stores and manages credentials for accessing secure Wi-Fi networks.
- Define SSID as it relates to Wi-Fi networks.
- Describe the purpose of SSIDs as they relate to Wi-Fi networks.
- Describe the features and purpose of ad-hoc networking as it relates to Wi-Fi networks on OS X computers.
- Describe the tools, options, and methods for configuring Wi-Fi.
- Describe the tools and methods for managing network locations.
- Describe the tools and methods for managing VPN connections.
• List the interfaces and interface protocols supported in a default installation of OS X.
• Describe how OS X computers acquire and use self-assigned (link-local) TCP/IP addresses on a network.
• Describe the ways to configure a network interface for 802.1X.
• Given a Mac with OS X installed, identify whether a network interface has received an IP address from a DHCP server or is using a link-local address.
• Use the Network Status pane of the Network preference.
• Given a Mac with OS X installed, identify the Ethernet or Airport MAC address.
• Use Network Utility.
• Given a Mac with OS X installed, identify a connection issue for a network interface.
• Use Ping in the Network Utility.
• List four common issues that can interrupt network services.
• Given a Mac with OS X installed, configure and manage multiple networks.
• Describe how network port priority affects network connectivity.
• Given a list of network interface priorities and active interfaces, identify the interface used for network access.

Lesson Twenty-two review questions
After completing Lesson Twenty-two, you should be able to answer the following questions.

1. What do the terms “interface,” “protocol,” and “service” mean in relation to computer networks?
2. What’s 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’s 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, and 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 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 whether outgoing data is destined for a network device on the LAN.

3. Most common IP addresses and subnet masks share the same IPv4 formatting. An IPv4 address is a 32-bit number represented in four groups of three-digit numbers, known as octets, separated by periods. Each octet has a value between 0 and 255. An IPv6 address is a 128-bit number that’s 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 whether the destination IP address is on the LAN. If the destination IP address isn’t 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 Twenty-three review questions

After completing Lesson Twenty-three, you should be able to answer the following questions.

1. What’s 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 Network preferences, how can you tell which interface is currently being used for network activities?

6. What’s the easiest method in 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 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:
   - 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
- USB connectivity via cellular network adapters or iOS devices with cellular network service
- 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

3. AppleTalk works only with OS X v10.5 or earlier.

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. So in most cases all WAN traffic, Internet traffic, and DNS resolution is sent through the primary network service interface.

5. In 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 to use a configuration profile containing all the relevant VPN setup information.

7. In 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 802.1X configuration profile provided by an administrator.

Lesson Twenty-four review questions

After completing Lesson Twenty-four, you should be able to answer the following questions.

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 can interrupt network services on a Mac are:
   - Ethernet connectivity issues, which 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, which prevent proper TCP/IP configuration
   - DNS service issues, which 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 isn’t 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.
Part Seven: Network Services

After completing Part Seven, “Network Services,” in OS X Support Essentials 10.9, you should be able to complete the following tasks. Five items from Part Seven are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Given a Mac with OS X installed, access network services.
- Identify the network services provided by iCloud on a Mac running OS X Mavericks.
- Describe the tools and methods used to configure network services for applications such as Safari, Mail, Messages, Contacts, Calendar, and Finder.
- Describe the tools and methods for configuring sharing services.
- Compare and contrast the tools and methods used for screen sharing.
- Given a Mac with OS X installed, sharing services configured, a network connection, and a scenario where sharing services aren’t working as expected, troubleshoot the configuration and connections to restore the service connection.
- Describe the tools and methods used to mount and unmount network share points.
- Use /Network to discover file services available on the network.
- Use the “Connect to Server” menu option in the Finder to access files from each of the five types of accessible file servers.
- Describe the relationship between client software, client configurations, server software, and server configurations relative to network service access.
- Describe the relationship between a network service and a network port.
- List three troubleshooting techniques for issues involving failure to connect to various network services.
- List the five types of file servers accessible via the “Connect to Server” menu option.
- List service discovery protocols supported by OS X.
- Describe how OS X uses dynamic service discovery protocols to access network services.
- Describe how items inside /Network in OS X are populated and organized.
- Describe common issues when connecting to file sharing services using OS X.
- List issues with metadata/file forks, and issues with connecting to file servers that don’t support AFP 3.1.
- Given a Mac with OS X installed, configure a firewall.
• Describe how firewalls work in OS X.
• Describe the advanced firewall settings in OS X.

Lesson Twenty-five review questions
After completing Lesson Twenty-five, you should be able to answer the following questions.

1. What's the relationship between clients and servers as it relates to 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 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. Internet Accounts preference is the primary interface in OS X for configuring built-in network applications.

4. From the “Connect to Server” dialog in the Finder, you can connect to:
   - Apple File Protocol (AFP)
   - Server Message Blocks/Common Internet File System (SMB/CIFS)
   - SMB2
   - Network File System (NFS)
• Web-based Distributed Authoring and Versioning (WebDAV)
• 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, and 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 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.

7. Review 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're 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 Twenty-six review questions
After completing Lesson Twenty-six, you should be able to answer the following questions.

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's 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's 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 devices. 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 won’t respond to any unsolicited connections).
Part Eight: System Management

After completing Part Eight, “System Management,” in *OS X Support Essentials 10.9*, you should be able to complete the following tasks. Twelve items from Part Eight are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Given a Mac with OS X installed, manage peripheral devices connected to a Mac.
- Given the System Information utility, identify 64- and 32-bit kernel extensions.
- Describe the tools and methods used to connect Bluetooth devices to an Mac running OS X Mavericks.
- Identify the buses supported by OS X to connect to and communicate with peripheral devices.
- Compare and contrast uses of the buses and their characteristics such as speed, power requirements, and connector types—including these buses: Bluetooth, SCSI, ATA, Serial ATA, FireWire, USB PC Card bus, Thunderbolt.
- Given the System Information utility identify connected peripherals and the buses they’re using.
- Use System Information.
- Define the term “device driver” as it applies to OS X.
- List three ways a device driver can be implemented in OS X.
- Given a Mac with OS X installed, configure the computer for printing and printer sharing.
- Describe the tools and methods used to configure printing on a Mac running OS X Mavericks.
- Describe the role of CUPS in OS X printing.
- Describe the role of PPD files in OS X printing.
- Discuss the steps that occur during the startup and sleep modes.
- Identify each of the processes that start up in OS X at system startup, in the order in which they launch.
- Map visual and audible cues to the stages of the OS X startup sequence.
- Describe the role of BootROM and the Power On Self Test (POST) in OS X startup.
- Describe the role of the launchd processes during OS X system initialization.
- Describe the role of startup scripts in the startup sequence of OS X.
- Describe the role of the login window process in user environment setup in OS X.
- Compare and contrast startup items with login items in OS X.
- Identify the stages of shutdown in OS X.
• Identify the stages of logout in OS X.
• Describe which types of computers and data are supported by the Power Nap feature in OS X.
• Identify the startup keyboard shortcuts and their functions in OS X.
• Describe the purpose and features of Verbose mode in OS X.
• Describe the purpose and features of Single-User mode in OS X.
• Given a Mac with OS X installed, troubleshoot and resolve issues related to OS X startup and shutdown.
• Describe methods for shutting down an unresponsive OS X computer.
• Describe how to identify and resolve kernel loading issues in OS X.
• Identify the location of files and scripts essential to the OS X startup process.
• Compare and contrast Safe Boot and Safe Mode.
• Identify the items that load when powering up in Safe Mode, in the order in which they load.
• Identify the keyboard combination to start a computer in Safe Mode.
• Describe how to further isolate and then resolve an issue that disappears when the computer is started up in Safe Mode.

Lesson Twenty-seven review questions
After completing Lesson Twenty-seven, you should be able to answer the following questions.

1. What are the four primary peripheral bus technologies supported by Mac computers 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’s 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 doesn’t 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,
   • Bluetooth wireless
2. Bluetooth devices must be paired to each other for communication to occur. Bluetooth preferences in the System Preference application is responsible for pairing your 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 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 instead of official third-party drivers.

5. If a connected peripheral doesn’t appear in System Information, the issue is likely to be hardware related. Troubleshoot accordingly.

Lesson Twenty-eight review questions
After completing Lesson Twenty-eight, you should be able to answer the following questions.

1. What does CUPS do?
2. What are PPD files responsible for?
3. What's the best source for acquiring printer drivers for OS X?
4. Under what circumstances can a standard (nonadministrative) user configure a printer?
5. How do you share printers with other users?
6. How can you select a new printer driver for a configured printer?
7. If it appears that all configured printers are having problems, what's a potential quick fix?

Answers

1. Common UNIX Printing System (CUPS) manages 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. Or 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 before the standard user configuring the printer.
5. You can enable printer sharing from 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. It depends on the printer. From Printing & Scanning preferences, sometimes you can simply select a new printer driver from the Options & Supplies dialog. In many cases though, to select a new printer driver for a configured printer you must delete and then re-add the printer.

7. If all printers appear to be having problems, 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 Twenty-nine review questions
After completing Lesson Twenty-nine, you should be able to answer the following questions.

1. What are the primary system initialization stages in OS X? What are the visual and audible cues of these items?

2. What does the firmware do? What’s 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 audible cues of these items?

6. What’s the difference between launch daemons, startup items, launch agents, and login items?

7. What are Safe Sleep and Power Nap?

8. What happens during user logout?

9. What happens during system shutdown?

10. Which keyboard shortcut is used to Safe Boot OS X?

11. Which keyboard shortcut can be used to temporarily choose another startup disk?

12. Which changes are made when OS X Safe Boots?

13. Which items aren’t loaded when OS X Safe Boots?

14. How do you further resolve an issue that disappears when the Mac successfully safe-boots?
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 the 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 computer’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.

10. A Safe Boot is initiated by holding down the Shift key during system startup.

11. Holding down the Option key at startup opens Startup Manager, which allows you to temporarily choose another startup disk.

12. A Safe Boot performs the following permanent actions: attempting to repair the system volume structure, deleting system KEXT caches, and deleting font caches.

13. When performing a Safe Boot, OS X doesn't 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.

14. If an issue disappears when a Safe Boot is successful, you must find and remove the third-party startup resource that caused the issue. The best way to isolate the problem 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.