12.10.3 Update Facts

Software, driver, and operating updates are an important part of your overall computer and network security. Many forms of malicious software, especially viruses and worms, operate by exploiting flaws in programs. It's important to know the difference between an update and an upgrade. Upgrades are usually new versions of software, such as Windows 7 to Windows 8. When there are releases for hotfixes and service packs, those are known as updates. When Windows released Windows 10 Anniversary Edition, that was considered an free upgrade and not an update. Windows has moved away from using the term Service Pack recently but the term is still used with other software developers.

Updates are periodically released to:

- Fix bugs (errors) in programming code
- Patch security vulnerabilities
- Add features or provide support for new hardware

Traditionally, updates came in two types depending on the software distribution:

Update Type	Description
Hotfix	A *hotfix* is an operating system patch that fixes bugs and other vulnerabilities in the software. ▪ Hotfixes may be released on a regular basis as fixes are created. ▪ For the highest level of security, apply hotfixes as they are released (after you use a test computer to verify that the hotfix will not cause additional problems). ▪ Microsoft identifies each hotfix by a number. This number also identifies a knowledge base (KB) article that describes the issues addressed by the hotfix.
Service Pack (SP)	A *service pack* (SP) is a collection of hotfixes and other system enhancements. ▪ A service pack includes all hotfixes released to that time. If you install the service pack, you do not need to install individual hotfixes. Installing a service pack also includes all previous service packs. ▪ Service packs might include additional functionality beyond simple bug fixes.

Windows Update is a feature of the Windows operating system that helps you keep your computer up to date.

- By default, Windows automatically checks for updates, downloads them, and installs them during the automatic maintenance window (which is 2:00 AM by default).
- Updates are classified as Important, Recommended, and Optional. By default, Important and Recommended updates are installed automatically.
- Windows Update can install both hotfixes and service packs. For example, after installing a new version of Windows, Windows Update will download and install the latest service pack.
- Windows Update includes updates for the following:
  - Windows operating system and utilities
  - Drivers that have passed Microsoft certification and that are made available through Windows Update
- For additional updates, you can use Microsoft Update in conjunction with Windows Update. Microsoft Update includes updates for Microsoft applications, such as Office applications.

You should be aware of the following facts when working with updates:

- Non-Microsoft applications and many drivers are not updated through Windows Update.
- To manually check for updates for applications or drivers, go to the manufacturer's website.
- Many applications include a feature that automatically checks the manufacturer's website periodically for updates. These programs typically ask your permission to install updates.
- Hardware devices, such as the BIOS or many networking devices, store code in a special hardware ROM chip. This software is referred to as *firmware*. Updates are done by *flashing* (replacing or updating) the code stored on the chip.
  - Always follow the instructions when performing firmware updates.
  - Many updates are performed through a browser; some updates can be performed only by booting to special startup disks while outside of Windows.
  - Turning off the device or interrupting the update process could permanently damage the device.
- Both hotfixes and service packs are specific to an operating system version.
- In a business environment, it is wise to test updates in an isolated lab environment (called a *sandbox*) before rolling them out to production systems.

Software usually has an end of life which is usually announced several months before the date it is no longer supported. For example, Windows XP and Server 2003 are no longer patched or updated. Once this happens, some of the dangers of end of life software could cause users to experience some of the following issues:

- Security vulnerabilities that are discovered by hackers.
- Software incompatibility where new software won't run on an older OS.
- Software not compliant with current regulations, such as hospitals and banking institutions.

- Higher cost of ownership. Some companies are paying software developers extra to maintain older versions of software to run on legacy operating systems.
- Poor performance due to aging hardware that the software is installed on.
