The Windows XP Professional Cram Sheet

This Cram Sheet contains the distilled, key facts about Windows XP Professional. Review this information as the last thing you do before you enter the testing center, paying special attention to those areas where you feel that you need the most review. You can transfer any of these facts from your head onto a blank sheet of paper immediately before you begin the exam.

INSTALLATION AND DEPLOYMENT

1. Know the differences between ACPI and APM when installing the OS, as well as the ramifications if the wrong one is in place after installation.
2. Know all the following processes for unattended and Remote Installation Service (RIS) installations:
   - *winnt.sif*—Used to automate CD-ROM-based installs.
   - *sysprep.inf*—The answer file for System Preparation (Sysprep) installs.
   - *winnt.exe with the /u, /s, and /udf switches*—Used for unattended installations.
   - *winnt32.exe and unattend.txt*—Automate an upgrade to Windows XP.
   - *Requirements for RIS are* Active Directory, DNS, and DHCP.
3. **winnt32.exe** with the checkupgradeonly switch are used to verify hardware and software compatibility before installation.
4. **rbfg.exe** is used to create remote boot disks for RIS clients if computers don't have network adapters with Pre-boot Execution Environment (PXE) boot ROM.
5. **riprep.exe** is used to create images of Windows XP Professional and applications for an RIS server.
6. **risetup.exe** is used to configure RIS.
7. **update.exe /s** is used to apply a service pack to a distribution share in slipstream mode.
8. Know how to convert to NTFS file system after installation, as well as how to stop the conversion after it has been initialized.
9. Remember that you can rollback to the old OS after Windows XP is installed in some circumstances, but never when upgrading from Windows 2000.
10. Know the details surrounding dynamic update for installation as well as the critical switches: **dudisable**, **dushare**, and **duprepare**.
11. Understand the sysprep tool and the essential switches that are available: **clean**, **factory**, **nosidgen**, and **reseal**.
12. Know the two important commands used with the User State Migration Tool: **scanstate** and **loadstate**.
13. Know the different "updates" that are available:
    - *Dynamic Update*—Used with installation to install the critical fixes and drivers.
    - *Automatic Updates*—Used with the Windows update feature and Web site to automatically download and offer critical fixes and drivers for the OS.
    - *Windows Update*—Built in service that helps control the critical fixes and drivers for the OS.

CONFIGURING AND MANAGING RESOURCES

14. The default for new shares is Everyone, Allow, Full Control. If share permissions conflict with NTFS permissions, the *most restrictive* permissions take precedence.
15. When you combine NTFS permissions based on users and their group memberships, the *least restrictive* permissions take precedence. However, Deny entries *always override* Allow entries.
16. By default, NTFS permissions are inherited from the parent folder. Permissions that are not inherited are referred to as *explicit.* Explicit permissions always override inherited permissions—an explicit Allow will even override an inherited Deny permission.
17. To change NTFS permissions on a file or folder, you must be the owner, or have the Change Permissions permission, which itself is part of Full Control. NTFS permissions are *retained* from the source folder whenever you *move* subfolders or files to another folder on the *same* NTFS volume. NTFS permissions are inherited from the destination folder in all other move and copy operations.
18. NTFS for Windows XP supports both file compression and data encryption. Encryption is implemented via the Encrypting File System (EFS). You can compress or encrypt a file, but not both.
19. Windows XP Professional and Windows 2000 computers can connect to printers that are attached to Windows XP, Windows 2000, and Windows .NET Server print servers through a Web browser. This feature uses the Internet Printing Protocol (IPP). IIS must be running on the machine you want to connect to. You can enter one of the following URLs into your Web browser:

    http://print_server_name/printers

    http://print_server_name/printer_share_name

SECURITY ACCOUNTS AND POLICIES

20. Local user and group accounts can be granted privileges and permissions to resources on the same system only. They cannot access resources on other systems.
21. Local user accounts can belong to local groups on the same system only. Domain user accounts can belong to global groups, universal groups, domain local groups, and machine local groups.
22. Renaming an account maintains all group memberships, permissions, and privileges of the account. Copying a user account maintains group memberships, permissions, and privileges assigned to its groups, but doing so does not retain permissions associated with the original user account. Deleting and re-creating an account with the same name loses all group memberships and permissions.
23. The most powerful group on a system is its local Administrators group. The Power Users group is an excellent group for most users that need to control the computer's resources, but not the computer's administration.
24. Organizational Units (OUs) in Active Directory create a hierarchical structure of containers for other objects, such as users, groups, and computers. Objects inherit attributes of their parent objects.
25. The Resulting Set of Policies (RSoP) is the final set of policies that is applied to the user and computer. The **gpresult** tool can help determine this RSoP, as can the **RSoP MMC snap-in**. The **gpupdate** tool can help "refresh" the policies to ensure the correct policies are applied.

MANAGING USER AND DESKTOP SETTINGS

26. Know the purpose and configuration of all the accessibility features: StickyKeys, FilterKeys Narrator, Magnifier, and On-Screen Keyboard.
27. Use the MSCONFIG utility to change system startup settings, enable and disable services, and modify BOOT.ini file settings.
28. The Regional And Language Options applet in Control Panel specifies user and input locales. It can also be used to add new input languages. Use this applet to pair input locales with a specific keyboard layout when a user needs to work with different languages.
29. Transfer data files and program settings from pre-Windows XP computers using either the User State Migration Tool (USMT) or the File Settings And Transfer (FAST) Wizard.
30. Applications can be deployed to users via a Group Policy. Applications can be either published or assigned. Install published applications via the Add and Remove Programs applet. Assigned applications have shortcuts in the Start menu, which will launch the installation program for an assigned application upon first use.
31. Typically, only applications compiled as an .msi file can be deployed via a Group Policy. However, non-.msi applications can use a ZAP file to tell Group Policy how to install the application.
32. To enable roaming profiles, enter the UNC path to the user's profile in the user's account properties.
33. To configure mandatory profiles, rename ntuser.dat to ntuser.man.
34. The Offline Files feature caches copies of network files locally. It is enabled by default on the client. On the server side, Manual Caching Of Documents is the default setting for shared folders. You can choose to Encrypt Offline Files To Secure Data from the Offline Files tab of the Folder Options dialog box.
35. Dualview is an advanced display option that enables a mobile computer to extend the Windows XP desktop onto both its built-in LCD display and onto an external monitor. It also supports desktop PCs that have on video adapter installed with 2 video output ports. You enable Dualview via the Display applet in Control panel.
36. Use the Program Compatibility wizard to run legacy applications in Compatibility Mode for Windows 95, Windows 98/Me, Windows NT 4 SP5, or Windows 2000. No other modes are available.

HARDWARE AND DEVICE DRIVERS

37. Windows XP can control whether users can install signed or unsigned drivers, or both, for a chosen device. The selection for this is called Driver Signing and is made as a Group Policy Object (GPO) settings for the Local Computer or as a Computer Configuration setting for a Windows Domain. The three choices for Unsigned Driver Installation Behavior are: Silently Succeed, Warn But Allow Installation, or Do Not Allow Installation. From the GUI, the choices are labeled Ignore, Warn, or Block.
38. To restore a device driver back to its previously installed version, open Device Manager, right-click the device you are having trouble with, and select Properties. Click the Driver tab and then click the Roll Back Driver button.
39. Power Options in Control Panel lets you customize your power scheme settings. Standby does not save your desktop state to disk; if a power failure occurs while the computer is on standby, you can lose unsaved information. The hibernate feature saves everything in memory to disk, turns off your monitor and hard disk, and then turns off your computer.
40. Windows XP Professional supports a maximum of 2 processors (CPUs).

DISK DRIVES, VOLUMES, AND FILE SYSTEMS

41. A Windows XP basic disk is a physical disk with primary and extended partitions. You can create up to three primary partitions and one extended partition with logical drives on a basic disk, or just four primary partitions. You cannot extend a basic disk.
42. A Windows XP dynamic disk is a physical disk that does not use partitions or logical drives. Instead, it has only dynamic volumes that you create using the Disk Management console. You can extend a volume on a dynamic disk. Dynamic disks can contain an unlimited number of volumes. Only Windows XP Professional (and Windows 2000) computers can directly access local dynamic volumes. However, computers that are not running Windows XP can access shared folders on dynamic volumes over the network.
43. You can convert a dynamic disk with volumes back to a basic disk, but you'll lose all your data. If you find yourself needing to do this, first backup your data, convert the disk to basic, and then restore your data.
44. Mounted drives, also known as mount points or mounted volumes, are useful for increasing a drive's "size" without disturbing it. Mount points also enable you to access multiple local storage devices through empty NTFS folders so that you don't have to assign drive letters. Drive paths are available only on empty folders on NTFS volumes. The NTFS volumes can be basic or dynamic.
45. Windows XP offers FAT (also known as FAT16) and FAT32 file system support with the following conditions or specifications:
    - Pre-existing FAT32 partitions up to 2 Terabytes are supported in Windows XP.
    - Windows XP allows you to create new FAT32 volumes of only 32GB or less.
46. Disk quotas track and control disk usage on a per-user, per-volume basis. You can apply disk quotas only to Windows XP NTFS volumes. Disk quotas do not use compression to measure disk space usage, so users cannot obtain or use more space simply by compressing their own data. To enable disk quotas, open the Properties dialog box for a disk, select the Quota tab, and configure the options.
47. To convert a volume from FAT or FAT32 to NTFS use **convert d: /fs:ntfs**. This command is one way and is not reversible. After the conversion, NTFS folder and file permissions for the root of drive volumes are set to Allow Read and Execute for the Everyone group.
48. Encrypted files that are moved or copied to another NTFS folder remain encrypted. Encrypted files that are moved or copied to a FAT or FAT32 drive volume become decrypted. If users (other than the one who encrypted the file or a user with shared access) attempt to move an encrypted file to a different NTFS volume, or to a FAT or FAT32 drive volume, they receive an Access Is Denied error message. If users other than the one who encrypted the file attempt to move the encrypted file to a different folder located on the *same* NTFS volume, the file is moved.

NETWORK PROTOCOLS AND SERVICES

49. TCP/IP is the default protocol suite. Its default setting is to obtain an IP address automatically. All IP addresses must have a subnet mask.
50. DHCP runs on Windows NT and Windows 2000 and .NET Server computers to automatically lease out dynamic IP addresses to client computers.
51. DNS is required for Active Directory. DNS provides name resolution by mapping host names to IP addresses and vice versa.
52. WINS is not required for Active Directory. WINS offers name resolution by mapping NetBIOS computer names to IP addresses and vice versa.
53. To troubleshoot TCP/IP connectivity problems, use the **ipconfig** and **ping** command-line utilities. The **ipconfig** tool displays the local computer's IP configuration; **ping** tests connectivity to remote computers and can test the local configuration by pinging the loopback address of 127.0.0.1.
54. Auto Private IP Addressing (APIPA) takes effect on Windows XP Professional computers if no DHCP server can be contacted. APIPA assigns the computer an IP address within the range of 169.254.0.0 through 169.254.255.254 with a subnet mask of 255.255.0.0.
55. Remote Assistance is the built in service which allows another user, typically a help desk or IT employee, to remotely help the end user with an issue that they are experiencing on their Windows XP Professional computer.
56. Remote Desktop is the built in service that allows you to access a session that is running on your computer while you are sitting at another computer.

TROUBLESHOOTING, MONITORING, AND SYSTEM RECOVERY

57. You can back up and restore files and directories with Windows Backup. You can launch this from the Accessories|System Tools Program group, the **ntbackup** command, or the properties sheet of any drive volume. Users can back up files to which they have at least the Read permission, and they can restore files to which they have at least the Write permission. To back up or restore other files, users need to be members of the Backup Operators group or the Administrators group.
58. Backing up the system state allows you to back up the registry, COM+ objects, and system startup files.
59. Know the following options for troubleshooting a system:
    - System Restore is the easiest way to return your computer to a previous state. Automatic restore points are set every 24 hours by default. You can also set your own manual restore points. Configure System Restore settings from the System Restore tab on the System Properties dialog box.
    - The Recovery Console is a special command prompt only mode you must boot the system into using the bootable Windows XP CD-ROM or by running **winnt32 /cmdcons** *before* a failure.
    - Safe Mode is generally the most useful troubleshooting mode because it starts the operating system with minimal services and drivers. It is best for removing services or drivers that are causing Stop Errors (aka "blue screens of death").
    - Last Known Good Configuration starts the system with the ControlSet (a portion of the registry) that was used the last time the system booted successfully and instantiated the Windows Explorer shell (desktop). If you install a driver or service that crashes *before you restart and log on again successfully*, you can restart the machine and select Last Known Good Configuration. Doing so effectively removes the driver or service from the active registry.
    - The Automated System Recovery (ASR) process is your *last resort* to recover the Windows XP operating system, the startup environment, and the registry. To use it, boot a system with the Windows XP Professional CD-ROM and choose the Repair option. You also need your most recent ASR floppy disk and your most recent ASR backup media set. The Windows Backup program (**ntbackup.exe**) is required for creating and restoring ASR backup media sets. .
60. Task Manager allows you to monitor particular performance metrics and to set the priority of applications. You should not select Realtime priority, which can interfere with other applications. Task Manager is also used to set processor (CPU) affinity for applications, but only on dual-CPU systems.
61. Use the Performance Console to monitor system performance and to establish baselines.
62. Logical disk counters for monitoring system performance do *not* need to be enabled using the **diskperf** command.

DIAL-UP AND RAS

63. IPSec negotiates encryption settings between the client and server to encrypt both passwords and data before an L2TP session is created.
64. EAP is an extension of Point-to-Point Protocol (PPP) for dial-up connections, and L2TP and PPTP clients. EAP supports several authentication protocols:
    - Message Digest 5 Challenge Handshake Authentication Protocol (MD5-CHAP)
    - Generic token cards
    - Transport Layer Security (TLS) for use with smart cards
65. Know well the default configurations for both dial-up and VPN connections with regard to the authentication, security, and encryption settings.
66. Internet Connection Sharing (ICS) uses the DHCP Allocator service to assign dynamic IP addresses to clients on the LAN within the range of 192.168.0.2 through 192.168.0.254. In addition, the DNS Proxy service becomes enabled when you implement ICS.
67. Internet Connection Firewall (ICF) is the service that monitors all aspects of the traffic that crosses the network interface, which includes inspecting the source and destination addresses, for further control. Typically port 80 (Web/HTTP), as well as ports 20 and 21 (FTP) are controlled.