Installing, Configuring and Administering

Microsoft Windows XP Professional

Version 3.1.0

Installing, Configuring, and Administering

Microsoft Windows XP Professional

Version 3.1.0

Abstract:

This study guide will help you to prepare for Microsoft exam 70-270, Installing, Configuring, and Administering Microsoft Windows XP Professional. Exam topics include Installation, Implementing & Administering Resources, Managing & Troubleshooting Hardware Devices, Monitoring & Optimization of System Performance & Reliability, Network Protocols & Services, and Implementing, Monitoring, & Troubleshooting Security.

Find even more help here:

Contents:

Installing Windows XP Professional

Requirements (KB# Q286463)

Component	Windows XP Home Edition	Windows XP Professional
Processors	1	1 or 2
Minimum CPU speed	233 megahertz (MHz)	233 MHz
Recommend CPU	300 MHz	300 MHz
Minimum RAM	64 megabytes (MB)	64 MB
Recommended RAM	128 MB	128 MB
Maximum RAM	4 gigabytes (GB)	4 GB
Disk Space for Setup	1.5 GB free	1.5 GB free

- All hardware should appear on the Windows Hardware Compatibility List (HCL) (KB# **Q142865**)
- Windows XP Professional supports Symmetric Multi-processing with a maximum of two processors, and up to 4 GB of RAM.

Attended installations

Setup stages

1. Setup Program (text mode)- preps hard drive for following stages of install and copies files needed for running Setup Wizard. Requires reboot. (Clean installations only.)
2. Setup Wizard (graphical mode) - prompts for additional info such as product key, names, passwords, regional settings, etc.
3. Install Windows Networking - detects adapter cards, installs networking components (Client for MS Networks, File & Printer Sharing for MS Networks), and installs TCP/IP protocol by default (other protocols can be installed later). Choose to join a workgroup or domain at this point (must be connected to network and provide credentials to join a domain). After all choices are made, components are configured, additional files are copied, and the system is rebooted.
4. Post installation – create user accounts and activate retail versions of Windows XP (customers using the Corporate Edition do not need to activate their product). This stage is sometimes referred to as the "Out of Box Experience" (OOBE).

Installing from CD-ROM

- Microsoft assumes that your system either has the ability to boot directly from a CD-ROM or that you will use a Windows 95/98/ME boot floppy to begin installing from a CD. The ability to create setup floppies has been dropped from Windows XP.
- If installing using an MS-DOS or Win95/98 boot floppy, run **winnt.exe** from the \i386 folder to begin Windows XP setup.
- Setup will not prompt the user to specify the name of an installation folder unless you are performing an unattended installation or using **winnt32** to perform a clean installation. (KB# Q222939)

Installing over a Network

- Create a distribution server that has a file share containing the contents of the \i386 directory from the Windows XP CD-ROM.
- Allocate 1.5 GB minimum plus 100 - 200 MB free hard drive space to hold temporary files during installation.
- Install a network client on the target computer or use a boot floppy that includes a network client (KB# Q142857). Run winnt.exe from a file share on the distribution server if installing a new operating system or **winnt32.exe** if upgrading a previous version of Windows.
- The client system must have a pre-existing FAT16 partition (MS-DOS & Win 95) or FAT32 partition (Win95 OSR2 & Win98) to hold setup files copied across the network.

Modifying Setup using Winnt.exe

Switch	Function
/a	Enables accessibility options.
/e[:command]	Specifies a command that will be run at the end of GUI-mode setup.
/r[:folder]	Specifies optional software to be installed. Folder is not removed after installation.
/rx[:folder	Specifies optional folder to be copied. Folder is deleted after installation.
/s[:sourcepath]	Specifies source location of Windows XP files. Can either be a full path or network share.
/t[:tempdrive]	Specifies drive to hold temporary setup files.
/u[:answer file]	Specifies unattended setup using answer file (requires /s).
/udf:*id*[,UDF_*file*]	Establishes ID that Setup uses to specify how a UDF file modifies an answer file.

Modifying Setup using winnt32.exe

Switch	Function
/checkupgradeonly	Checks system for compatibility with Windows XP. Creates reports for upgrade installations.
/cmd:*command_line*	Instructs Setup to carry out a specific command before the final phase of setup. Occurs after computer has restarted but before setup is complete.
/copydir:*folder_name*	Creates additional folder inside %systemroot% folder. Retained after setup.
/copysource:*folder_name*	Same as above except folder and its contents are deleted after installation completes.
/cmdcons	This adds a Recovery Console option to the operating system selection screen.
/debug[*level*] [:*file_name*]	Creates a debug log. 0=sever errors only. 1=regular errors. 2=warnings. 3=all messages.
/dudisable	Prevents Dynamic Update from running. Will override an answer file with a Dynamic Update option specified.
/duprepare: *pathname*	Prepares an installation share to a copy of files downloaded by Dynamic Update from the Windows Update Web site. This share can be used for subsequent XP installations rather than having the machines contact Windows Update.
/dushare: *pathname*	Specifies a share that Dynamic Update files have been previously downloaded to.
/m:*folder_name*	Forces Setup to look in specified folder for setup files first. If files are not present, Setup uses files from default location.
/makelocalsource	Forces Setup to copy all installation files to local hard drive so that they will be available during successive phases of setup if access to CD drive or network fails.
/nodownload	Used when upgrading from Win95/98. Forces copying of winnt32.exe and related files to local system to avoid installation problems associated with network congestion. (KB# Q244001)
/noreboot	Tells system not to reboot after first stage of installation.

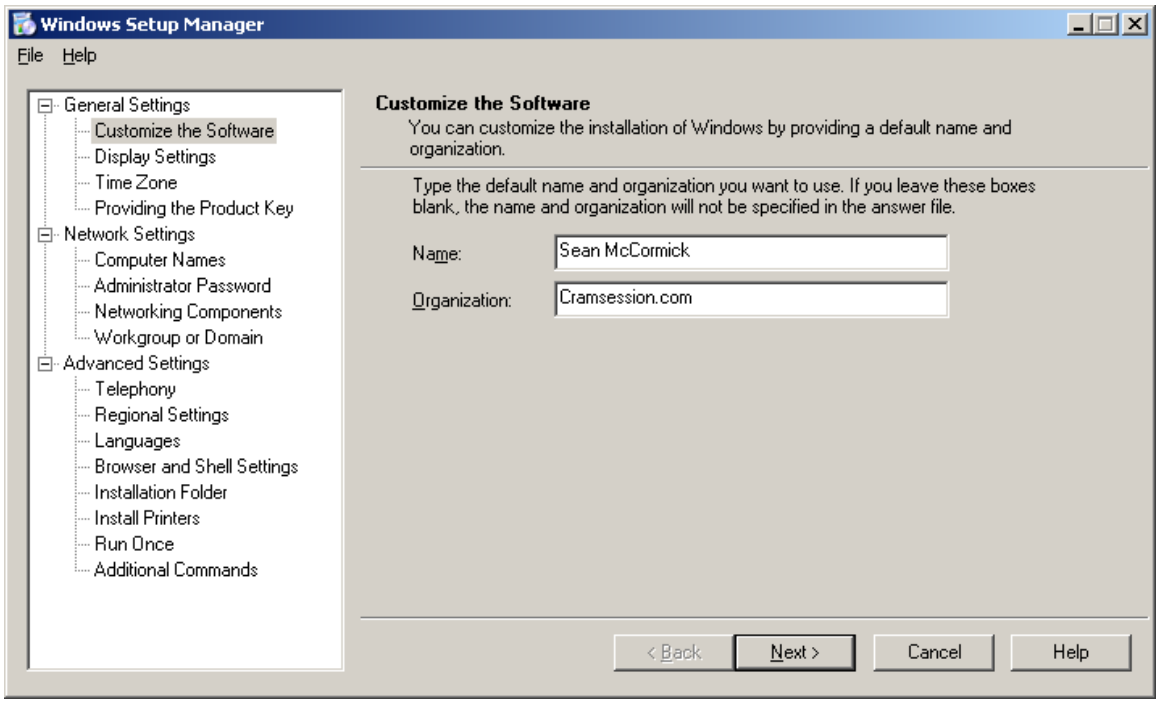
/s:*source_path*	Specifies source path of installation files. Can be used to simultaneously copy files from multiple paths if desired (first path specified must be valid or setup will fail, though).
/syspart:*drive_letter*	Copies all Setup startup files to a hard disk and marks the drive as active. You can physically move the drive to another computer and have the computer move to Stage 2 of Setup automatically when it is started. Requires /tempdrive switch. (KB# Q234037 & Q241803)
/tempdrive:*drive_letter*	Setup uses the specified tempdrive to hold temporary setup files. Used when there are drive space concerns.
/unattend: [number] [:*answer_file*]	Specifies answer file for unattended installations.
/udf:id[,*udf_file*]	Establishes ID that Setup uses to specify how a UDF file modifies an answer file.

Unattended installations

Working with Answer Files

- Unattended installations rely on an *answer file* to provide information during setup process that is usually provided through manual user input. (KB# Q183245)
- Answer files can be created manually using a text editor or by using the Setup Manager Wizard (SMW) which is shown in Figure 1.

- Figure 1 – The Setup Manager Wizard



- SMW can be found on the Windows XP Professional CD in the \SUPPORT\TOOLS folder in a file called DEPLOY.CAB. Extract these to a folder on your hard drive.
- SMW allows for creation of a shared Distribution Folder and OEM Branding
- If you had a CD in drive D:\ and an unattended installation answer file named salesans.txt in C:\, you could start your install with this command: **D:\i386\winnt32 /s:d:\i386 /unattend:c:\salesans.txt** (KB# Q216258)
- There are five levels of user interaction during unattended installs:

    1. *Provide Defaults* - Administrator supplies default answers and user only has to accept defaults or make changes where necessary.
    2. *Fully Automated* - Mainly used for Win2000 Professional desktop installs. User just has to sit on their hands and watch.
    3. *Hide Pages* - Users can only interact with setup where Administrator did not provide default information. Display of all other dialogs is suppressed.

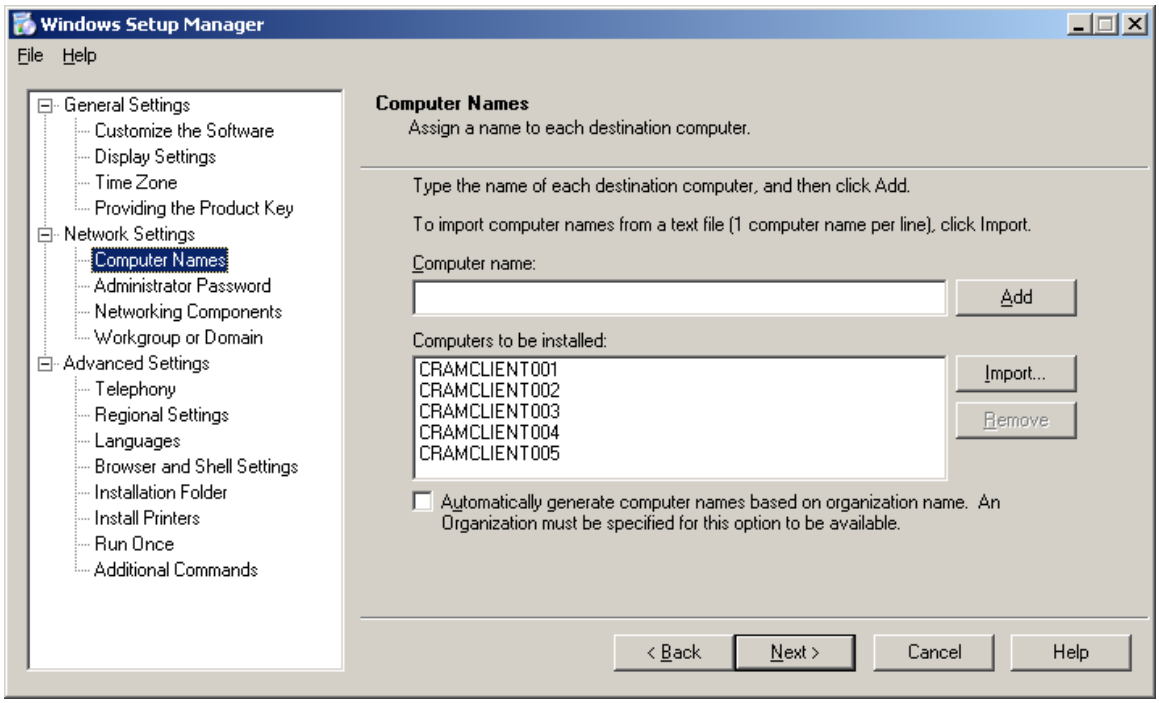
4. *Read Only* - Similar to above, but will display information to user without allowing interaction to pages where Administrator has provided default information.
5. *GUI Attended* – User has some interaction with the setup program. Text mode is automated; user must respond to screens in the setup wizard.

- When performing an unattended installation using the XP Product CD, you must name your answer file **winnt.sif** and place it in the root directory of a floppy disk inserted into drive A: of your computer. Setup will automatically locate the **winnt.sif** file and process it so long as it is named correctly.
- The **sysdiff** tool for installing software applications as part of unattended installations is not supported in Windows XP. You will need to use Group Policy to deploy software or a software management tool such as Systems Management Server.
- You can enter the CD product key manually under the *[UserData]* section of the answer file:
  ProductID="XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
- You can activate a retail version of Win XP under the *[Unattended]* section of the answer file:
  AutoActive=Yes (KB# Q291997)

Creating Uniqueness Database Files (UDF)

Answer Files are only useful for installing one machine at a time. If you're installing 50 machines in one go and you want each one to have a unique identity on the network, you will have to create fifty separate Answer Files – that's a lot of work. Instead of creating a separate Answer File for each installation, an easier way to go about things it to create a Uniqueness Database File (UDF). The UDF file is used in conjunction with the Answer File and can provide multiple answers for installations done from a single Answer File.
UDFs provide keys and values for each machine that are used to replace corresponding keys and values in an Answer File. When you start the unattended installation you will provide an ID for the machine being installed so that Setup knows which section of the Uniqueness Database File to use.
The Setup Manager Wizard creates a UDF automatically whenever you enter more than one computer name, as shown below in Figure 2.

Figure 2 – Entering multiple Computer Names into the Setup Manager Wizard



Here is the Uniqueness Database File that the Setup Manager Wizard created using the input shown above:

```
;SetupMgrTag
[UniqueIds]
   CRAMCLIENT001=UserData
   CRAMCLIENT002=UserData
   CRAMCLIENT003=UserData
   CRAMCLIENT004=UserData
   CRAMCLIENT005=UserData
[CRAMCLIENT001:UserData]
   ComputerName=CRAMCLIENT001
[CRAMCLIENT002:UserData]
   ComputerName=CRAMCLIENT002
[CRAMCLIENT003:UserData]
   ComputerName=CRAMCLIENT003
[CRAMCLIENT004:UserData]
   ComputerName=CRAMCLIENT004
[CRAMCLIENT005:UserData]
   ComputerName=CRAMCLIENT005
```

You will need to specify the ID of the system being installed as well as the location of the UDF file in the form of a switch when performing an unattended installation. Here is an example of what an installation from a command line would look like:

winnt /s:\\CORPSVR5\I386 /u:\\CORPSVR5\ANSWR\unattend.txt /udf:CRAMCLIENT001,\\CORPSVR5\ANSWR\udf.udb

How UDF files are processed

The keys and values specified in a Uniqueness Database File will always override a corresponding section in an Answer File. The Answer File may override a key that is not specified or assigned in the UDF resulting in the user performing the installation being prompted for input. The scenarios and their results are shown in the table below:

UDF	Answer File	Result
Key not specified	Key + value specified	Value from Answer File used
Key specified, value not specified	Key not specified	No value configured – user may be prompted for info
Key + value specified	Key not specified	Value in UDF used
Key + value specified	Section or key not specified	Section + key configured by Setup
Key + value specified	Key not specified	Value in UDF used

If the UDF is specified on the command line with **winnt** or **winnt32** it can be given any name. However, if you specify the ID of the computer on the command line but fail to specify the name of a UDF file, you will need to supply the UDF on a 3.5-inch floppy disk using a specific name. The file must be named **$Unique$.udf** or setup will not be able to locate it and the user is prompted for it.

Deploying WinXP by using Remote Installation Services (RIS)

Overview:

Remote Installation Services (RIS) is used to lower the Total Cost of Ownership (TCO) of Windows by simplifying the process of installing new client workstations. You can install Windows 2000 Professional and Windows XP Professional clients using RIS.
It's also possible to deploy both Windows 2000 Server (CD-based images only – KB# Q214794) and Windows XP Home edition using RIS (CD-based and RIPrep images – KB# Q305308), but Microsoft does not support or recommend doing either.

RIS Server requirements:

- DHCP Server Service
- Active Directory
- DNS Server Service

- At least 2 GB of disk space. Hard disk must have at least two partitions, one for the Operating System and one for the images. Image partition must be formatted with NTFS. RIS packages cannot be installed on either the system or boot partitions. They also cannot be on an EFS volume or DFS shared folder.

Steps for setting up RIS Server:

- Install Remote Installation Services using **Control Panel > Add/Remove Programs > Windows Components**.
- Start the RIS Setup Wizard by running **risetup**. Specify the *Remote Installation Folder Location*. For *Initial Settings*, choose *Do not respond to any client requests* (default setting - RIS Server must be authorized first). Specify the location of the WINXP Professional source files for building the initial CD-based image. Designate a folder inside the RIS folder where the CD image will be stored. Provide a friendly text name for the CD-based image.
- Setup Wizard creates the folder structure, copies needed source files to the server, creates the initial CD-based WINXP Professional image in its designated folder along with the default answer file (Ristandard.sif), and starts the RIS services on the server.
- Server must now be authorized. Open **Administrative Tools > DHCP**. Right-click DHCP in the console tree and choose *Manage authorized servers*. When dialog appears, click *Authorize* and enter name or IP of the RIS server (user must be a member of the Enterprise Admins group to do this).
- You may now configure your RIS Server to respond to client requests.
- Assign users/groups that will be performing RIS Installations permissions to Create Computer Objects in Active Directory.
- The Client Computer Naming Format is defined through Active Directory Users & Computers. Right-click the **RIS Server** and click **Properties > Remote Install > Advanced Settings > New Clients**. Choose a pre-defined format or create a custom one. Variables are: %Username (user logon name), %First (user first name), %Last (user last name), %# (incremental number), %MAC (NIC hardware address). (KB# Q244964)
- Associate an answer file (.SIF) with your image.

Creating a RIPrep Image

- Procure a source computer and install Windows XP Professional. Configure all components and settings for your desired client configuration, keeping everything on a single partition (RIPrep Wizard can only image a single partition).
- Install your applications and configure them. Do not install unnecessary applications - remember that RIS requires Active Directory, which can be used to publish or assign software as needed using Group Policy.

- As you created and configured the system using the Administrator profile, you will need to copy your configuration to the Default User profile so that your custom settings will not be lost.
- To launch the RIPrep Wizard, click **Start > Run** and type the following into the Open box: *RISServerName***reminst\admin\i386\riprep.exe**. Provide the name of the RIS Server where the image will be stored, the folder that will hold the image, and a friendly text description.

RIS Client requirements: (KB# Q228908)

- Client machine must meet minimum hardware requirements for Windows XP Professional and clients receiving RIPRep images must use the same Hardware Abstraction Layer (HAL) as the image file.
- Must have a network adapter that meets the Pre-boot Execution Environment standard (PXE) version 99c and higher (there is a confirmed problem with v99j - KB# Q244454) or a 3 1/2" floppy drive and PCI network adapter supported by the RIS Startup Disk utility's list of supported adapters. (KB# Q244036 & Q246184)

Comparing RIPrep images with CD-based images

RIPrep Image	CD-based image
Can only be deployed to a computer with the same HAL as the source computer.	Can be deployed to ANY computer with a HAL supported by WINXP.
Contains the OS and applications.	Contains the Operating System only and applications are deployed separately using Group Policy.
Created manually.	Created automatically upon installation of RIS Server.
Based on a pre-configured client computer. Cannot be changed without recreating the image. Separate image required for each installation type.	Based on default settings of operating system. An image file is used to customize the image. Multiple answer (.SIF) files can be used to customize the same image.
Only necessary files and registry keys are copied to the client system. Fastest method.	All files are copied to client hard drive before Setup program is started. Slower and places and additional burden on a network.

Troubleshooting Remote Installations

- If computer displays a BootP message but doesn't display the DHCP message, check to see if it can obtain an IP address. If it cannot, make sure a DHCP server is online, is authorized, has a valid IP address scope, and that the DHCP packets are being routed (you may need to install a DHCP relay agent if

your DHCP server is located on a different network segment than the RIS client –(KB# Q174765)

- Computer displays the DHCP message but does not display the Boot Information Negotiations Layer (BINL) message. Make sure the RIS server is online and authorized and that DHCP packets are being routed. (KB# Q235979)
- BINL message is displayed but system is unable to connect to RIS server. Try restarting the NetPC Boot Service Manager (BINLSVC) on the RIS Server.
- If the Client cannot connect to RIS Server using the Startup disk, check to make sure you used the right network adapter driver in **rbfg.exe**.
- If the installation options you expected are not available, there may be Group Policy conflicts. Check to make sure another Group Policy Object did not take precedence over your own.
- If a PXE client displays the message "Operating system not found" configure the system to boot from the network in its BIOS settings.
- If a valid RIPrep image is not displayed in the list of installation choices it may be because it was created using a particular Hardware Abstraction Layer (HAL) and you are attempting to install it to a platform with an incompatible HAL. If you wish to deploy an image to a system with a different HAL you must recreate it using the correct HAL – changing the *HalName* value in the Riprep.sif file alone is not sufficient. (KB# Q289638)
- While it is *technically* possible to deploy the Home Edition of Windows XP using RIS, Microsoft doesn't support it and is offended by the idea because you're robbing them of much needed licensing dollars. (KB# Q305308)
- If you can't find the right driver for your network card in RBFG.EXE you can add one manually if it has been digitally signed. (KB# Q246184)

Miscellaneous:

- You cannot create RIPrep images on a server unless it already has an existing CD-based image.
- The Remote Boot Floppy Generator utility (**rbfg.exe**) only works on Windows 2000 and Windows XP systems (KB# Q246618). To create boot floppies, click **Start > Run** and then type:
  *RISServerName***reminst\admin\i386\rbfg.exe**
  and click OK
- The answer file (.SIF) supports the new [RemoteInstall] section. Setting the repartition parameter to yes causes the install to delete all partitions on the client computer and reformat the drive with one NTFS partition.
- Pre-staging images using the GUID of PXE-based workstations prevents unauthorized users from illegally installing Windows XP onto their systems.
- The MAC address of the network adapter can be entered into the GUID field and padded with zeros.

System preparation tool (SYSPREP.EXE): (KB# Q302577)

- Removes the unique elements of a fully installed computer system so that it can be duplicated using imaging software such as Ghost or Drive Image Pro. Avoids the NT4 problem of duplicated SIDS, computer names etc. Installers can use Sysprep to provide an answer file for "imaged" installations.
- Target computers must have the same Hardware Abstraction Layer (HAL) as the original cloned computer and use the same disk controller type.
- **sysprep.exe** must be extracted from DEPLOY.CAB in the \support\tools folder on the Windows XP Professional CD-ROM.
- Adds a mini-setup wizard to the image file that is run the first time the computer it is applied to is started. Guides user through re-entering user specific data. This process can be automated by providing a script file. (KB# Q196667)
- Use Setup Manager Wizard (SMW) to create a SYSPREP.INF file. SMW creates a SYSPREP folder in the root of the drive image and places sysprep.inf in this folder. The mini-setup wizard checks for this file when it runs. (KB# Q216937)
- Specifying a CMDLINES.TXT file in your SYSPREP.INF file allows an administrator to run commands or programs during the mini-Setup portion of SYSPREP. (KB# Q238955)
- If you want to activate a copy of Windows XP through Sysprep you will need to do so through an answer file.

Sysprep switches

Switch	Function
-activated	Tells Sysprep NOT to reset the grace period for Windows Product Activation – only used if system was activated in the factory.
-audit	Reboots system into Factory mode without generating new SIDS or processing the [OEMRunOnce] section of winbom.ini. Used only when the system is already in factory mode.
-clean	Cleans the critical devices database used by the [SysprepMassStorage] section of Sysprep.inf.
-factory	Forces restart in network-enabled state and bypasses Windows Welcome (OOBE) and mini-setup screens. Used for updating drivers, running plug and play, and configuration in a factory environment.
-forceshutdown	Forces the computer to shutdown after Sysprep is complete.
-mini	Forces Windows XP to use the mini-setup wizard the first time it is started after running Sysprep (Corporate Edition only – the Home Edition always goes to the Windows Welcome screen).
-msoobe	Forces Windows XP to use the Windows Welcome screen (also called Out Of Box Experience, or OOBE) the first time it is started after running Sysprep.
-noreboot	Used to modify registry keys without forcing a reboot at the end of Sysprep for testing purposes only. Do not use in a production environment.

-nosidgen	Tells Sysprep not to generate new SIDS. Used only when NOT duplicating the computer Syprep is being run on or when pre-installing Domain Controllers.
-pnp	Forces full Plug and Play device enumeration when used with the mini-setup wizard. Cannot be used with Windows Welcome.
-quiet	Forces Sysprep to run without displaying confirmation messages or dialogs on screen. Used in conjunction with unattended installations.
-reboot	Forces reboot at the end of Sysprep so that Syprep can be verified before system is resealed and delivered to customer.
-reseal	Used to prep system for delivery to customer. This will wipe Event Viewer logs. This is the last step in using Sysprep.

- There are four modes that have been added to Sysprep under Windows XP: (KB# Q282190)

    1. *Audit* – lets a system builder boot up and verify that the operating system is configured properly while running in factory floor mode.
    2. *Factory* – used to customize a pre-install on the factory floor by using a Bill of Materials file to automate software installations, software, and driver updates, updates to the file system, the registry, and INI files such as Sysprep.inf. Invoked via the **sysprep -factory** command.
    3. *Reseal* – used by an OEM after running Sysprep in factory mode to prepare a system for delivery to a customer. Invoked using **sysprep –reseal** command. You can send the customer to the mini-setup wizard or OOBE screen by using the **–mini** and **–msoobe** switches respectively.
    4. *Clean* – Used to clean out the critical device database. Only those devices installed in the computer are left intact. Invoked using the **sysprep –clean** command.

Performing Upgrades: (KB# Q232039)

Upgrade paths

The following operating systems can be directly upgraded to Windows XP Professional. The setup routine will preserve and migrate all possible software and settings:

- Windows 98
- Windows Millennium Edition
- Windows NT 4.0 with Service Pack 6
- Windows 2000 Professional

Earlier versions of Windows must be upgraded to a supported operating system first before upgrading to Windows XP Professional:

- Windows 95 → Windows 98
- Windows NT earlier than NT4 SP6 → Windows NT4 SP6

Before upgrading

Microsoft suggests performing the following steps before upgrading a system to Windows XP:

- Make sure all hardware in the system appears on the Hardware Compatibility List (HCL) at http://www.microsoft.com/hcl.
- Ensure hardware meets the minimum system requirements.
- Run the Windows Readiness Analyzer and generate a Compatibility Report to make sure that all hardware and software is supported on the system being upgraded. Use **winnt32 /checkupgradeonly** to run the Windows Readiness Analyzer.
- Backup all files.
- Scan for viruses and then disable antivirus software as it may interfere with the upgrade process.
- Uncompress any compressed drives. The only compressed drives that can be safely upgraded are the ones using NTFS file system compression.
- If you are upgrading an NT4 system using spanned or striped sets, you must backup the data, delete the spanned or striped sets in Disk Manager, upgrade to XP, convert the disk to Dynamic (covered later), create spanned or striped volumes, and then restore backed up data.

Performing the upgrade

- Insert the XP product CD and run **winnt32.exe** from the \i386 directory to upgrade from a previous version of Windows or select **Upgrade to Windows XP Professional (Recommended)** from the autorun dialog that may appear after the CD is inserted. (KB# Q199349)
- Upgrade installations from a network file share are not supported in Windows XP (this *can* be done, but only by using SMS). You must either do a CD-based upgrade or perform a clean installation of Windows XP and re-install needed applications.
- Because of registry and program differences between Win95/98 and XP, upgrade packs (or migration DLLs) might be needed. Setup checks for these in the \i386\Win9xmig folder on the Windows XP CD-ROM or in a user specified location. (KB# Q231418)
- Run **winnt32 /checkupgradeonly** to check for compatible hardware and software without starting the installation process. This procedure generates a report indicating which system components are Windows XP compatible.

Upgrade types

You will be presented with two upgrade options, Express and Custom. Here are the differences:

- *Express upgrade* – upgrades Windows installation using current system folder (e.g. c:\winnt) and maintains all current settings. MS recommends using the Express upgrade.
- *Custom upgrade* – this allows you to modify the installation folder, language options, and gives you an opportunity to upgrade file systems formatted with FAT or FAT32 to NTFS.

Upgrade Gotchas

- With Windows 98/ME upgrades, Windows XP provides you with an opportunity to uninstall the new operating system and revert to the old one, but only if you maintain the current FAT or FAT32 file systems. Converting your file system to NTFS will remove this uninstall option.
- You will receive an Upgrade Report as part of the upgrade process. Most warnings will involve specific software programs. You will most likely be able to run this program using Compatibility Mode and can safely continue with the upgrade in most instances.
- The version of the NTFS file system used by Windows NT 4 is automatically upgraded to the version of NTFS used by Windows XP. Custom filters created for the older version of NTFS (used by some anti-virus software) may stop working under Windows XP.

Uninstalling Windows XP

- To uninstall Windows XP from an upgraded system, navigate to the **Add/Remove Programs** applet in **Control Panel**, highlight **Windows XP**, and click the **Change/Remove** button.
- You cannot uninstall Windows XP if you have converted your FAT partition to NTFS, or upgraded from Windows NT 4 Workstation or Windows 2000 Professional.
- Programs that have been modified since the upgrade to Windows XP may not function properly after the un-installation, particularly if they hook into registry settings unique to Windows XP.

Dynamic Update

Dynamic Update is a cool new feature that is only found in Windows XP. In a nutshell, it lets you connect directly to a network source, either the Windows Update site or a shared folder on your own network, to find critical fixes and drivers needed to minimize setup difficulties. There are some caveats…

- Dynamic Update needs an Internet connection or the ability to connect to a network share containing updates that were previously downloaded from the Windows Update Corporate Catalog.
- For upgrade installations, the version of Windows being upgraded must contain the WINENET.DLL and SHLWAPI.DLL files from Internet Explorer 4.01 or later (this may affect some Windows NT 4 Workstation systems that never had a recent browser installed because they weren't used for Web access).
- Dynamic Update takes place by default when performing an unattended upgrade, but can be disabled by adding the following key and value to your answer file: DUDisable=yes.
- You can disable Dynamic Update by using the /dudisable switch. This will also override and answer file that is set to allow Dynamic Update.
- You can minimize traffic on your outbound Internet connection by downloading update files from the Corporate Windows Update site and mounting them on a network share (e.g. \\CORPSVR5\DYNUPDATE) and using the switch:
  winnt32.exe /dushare: \\CORPSVR5\DYNUPDATE for an upgrade installation.
- The /dushare switch (used in conjunction with the /duprepare switch) can be used to copy all files downloaded by Dynamic Update to a network share for use by subsequent installations. You must create a shared folder on a server ahead of time.

Dynamic Update downloads consists of two types of files:

1. Device Drivers – These are only downloaded for devices that are connected to the computer but for which there is no existing driver on the CD-ROM or distribution point. If there is an existing driver already, the updated version will not be downloaded unless it has been tagged as a "critical fix".
2. Replacement Files – Dynamic Update checks to see if there are any critical fixes or updates for files currently available on the installation CD or distribution point. Updated files are downloaded, but any new files that don't appear on the CD are ignored.

Dual-booting Windows XP with other Operating Systems

MS-DOS, Windows 3.x, and Windows 95/98/ME

These operating systems face the following limitations when dual-booted with Windows XP:

- The active partition that the computer is started from must be formatted with a file system that is recognized by these legacy operating systems. MS-DOS, Windows 3.x, and Windows 95 use the FAT file system. Windows 95 OSR2, Windows 98, and Windows ME use both the FAT and FAT32 file systems. None of these operating systems recognize the file system – you cannot format the active partition with the NTFS file system without rendering older operating systems unbootable.
- Partitions formatted as NTFS cannot be accessed by these operating systems.
- These operating systems must be installed *before* Windows XP.
- Neither MS-DOS, Windows 3.x, nor Windows 95/98/ME are compatible with Dynamic Disks.

Windows NT 4

Here are some things to be aware of when dual-booting Windows NT and Windows XP:

- When Windows XP is installed on a computer running Windows NT 4 all existing NTFS partitions will be updated to the version of NTFS used by Windows XP.
- For your Windows NT 4 configuration to access the upgraded NTFS volumes it must be running Service Pack 4 or higher. This service pack allows it to read the NTFS volumes without giving NT4 access to newer features such as Encrypting File System, Disk Quotas, Volume Mount Points, etc.
- Windows NT 4 cannot access disks that have been converted to Dynamic.

Windows 2000

Here are issues to be aware of when using Windows 2000 and Windows XP in a dual-boot scenario:

- Both Windows 2000 and Windows XP can access Dynamic Disks, but a set of Dynamic Disks can only belong to one operating system at a time. Never use Dynamic Disks in a dual-boot scenario.
- Systems participating in a Windows 2000 or Windows XP security domain must have different computer names.

Migrating User Settings

File and Settings Transfer Wizard (FAST)

This is a GUI tool that allows a user upgrading their system to migrate their files and settings over to Windows XP. It is intended for situations where a single computer is being upgraded or the computer's owner is performing the upgrade.
Because this tool only exists on systems running Windows XP you will need to run it from the XP product CD, use a direct cable connection between systems, or create a Wizard disk on a 3.5-inch floppy disk.
You can choose to copy the files being transferred to either large removable media or a shared network location.
To run the Wizard from the XP product CD run **fastwiz.exe** from the \SUPPORT\TOOLS directory.
To run the Wizard from a newly created Wizard disk, click **Start > Run** and then type **a:\fastwiz.exe**.
The user can now select the files and settings they wish to transfer using the wizard and move them to the shared network location or to the removable media.

User State Migration Tool (USMT)

This is a command line tool that is used to help administrators migrate settings from systems running Windows 95, Windows 98, and Windows ME over to Windows XP. This tool is not used with Windows 2000. This works with the most popular Microsoft software applications by default but can be customized to work with other applications. USMT can be scripted and is used for mass deployments.

File types transferred by default

.ch3	.dot	.oqy	.ppt	.scd	.wps
.csv	.dqy	.pot	.pre	.sh3	.wq1
.dif	.iqy	.ppa	.rqy	.txt	.wri
.doc	.mcw	.pps	.rtf	.wpd	.xls

Folders transferred by default

- Desktop
- Favorites
- My Documents
- My Pictures

Windows settings transferred by default

- Accessibility Options
- Browser/Mail Settings
- Display Settings
- Folder/Taskbar Options
- Fonts
- Mapped Network Drives
- Mouse/Keyboard Settings
- Network Printers

Application settings transferred by default

- Microsoft Access
- Microsoft Excel
- Microsoft Office
- Microsoft Outlook
- Microsoft PowerPoint
- Microsoft Word
- Stored Mail and Contacts

Preparing a server for USMT

1. Create a shared folder called USMT.
2. Give the migrating user read access to USMT and the Admin account on the destination computer read/write access.
3. Create another folder called MigStore – share it with the same name. Both the migrating user and admin account on the destination computer require read/write access.
4. Create a sub-folder in USMT called Scan.
5. Create a sub-folder in USMT called Load.
6. Insert the Windows XP product CD and copy these files from \VALUEADD\MSFT\USMT to \USMT\SCAN; **scanstate.exe, *.inf, *.dll**.
7. Copy the following files from \VALUEADD\MSFT\USMT to \USMT\SCAN; **loadstate.exe, *.dll, MigUser.inf**.

Scanning the source computer

1. Log on as migrating user.
2. Map a drive to USMT folder on server.
3. From a command prompt, go to USMT/Scan folder on server.
4. Run **scanstate.exe** using this command line:
   scanstate /i .\migapp.inf /i .\migfiles.inf /i .\sysfiles.inf *servername*\MigStore
5. Once the program has finished running move to the destination computer.

Migrating files to destination computer

1. Log on as Admin, not migrating user.
2. Make sure migrating user does not have an account on destination computer.
3. Map drive to USMT folder on server.
4. From command prompt go to USMT/Load folder.
5. Run **loadstate.ext** using this command line:
   loadstate /i .\miguser.inf *servername*\MigStore
6. When program finishes, logon as migrating user to verify successful migration. Classic Windows shell should appear, as it is part of migration.

Product Activation

To reduce the amount of software piracy it has to cope with, especially "casual copying" amongst home users, Microsoft has introduced Product Activation. Product Activation essentially ties your Windows software to specific computer hardware, preventing you from installing the same copy of Windows on multiple computers. After installing Windows XP, you have 30 days in which to activate your product with Microsoft. This can be done over the Internet or via a phone call.
Once your copy of Windows is activated you won't have to worry about this feature again unless you have a habit of changing your hardware around frequently. Windows XP puts special weight on your computer's network adapter. If you don't change your NIC, you can change up to five items without having to re-activate. If your computer doesn't have a NIC, or you change your NIC, you're allowed up to three hardware changes before you have to re-activate your operating system.
If you suffer a catastrophe and have to re-install Windows XP from scratch, you won't have a problem with Product Activation unless you've changed your hardware around a bit. Then you'll be informed that your copy of Windows is already registered to another system and will have to phone up Microsoft and beg and plead a bit. Microsoft allows up to four activations a year for people who like to tinker with their systems. After that, who knows?
This is obviously an annoying feature to cope with, especially in large corporate environments where deployments are done on a large scale. Microsoft offers volume licensing for large corporations. Those corporations participating in this Volume Licensing Plan can obtain a Corporate Edition of Windows XP Professional that only requires a valid product key, but not Product Activation.
You can activate your copy of Windows XP Professional at the Windows Welcome Screen, by choosing **Start** > **Activate Windows**, or by typing **oobe/msoobe /a** at a command prompt.
Product activation uses TCP/IP ports 80 (HTTP) and 443 (HTTPS).

Troubleshooting failed installations

Common errors

Problem	Possible fix
Cannot contact domain controller	*Verify that network cable is properly connected.* Verify that server(s) running DNS and a domain controller are both on-line. Make sure your network settings are correct (IP address, gateway, etc.). Verify that your credentials and domain name are entered correctly.
Error loading operating system	Caused when a drive is formatted with NTFS during setup but the disk geometry is reported incorrectly. Try a smaller partition (less than 4 GB) or a FAT32 partition instead.
Failure of dependency service to start	Make sure you installed the correct protocol and network adapter in the Network Settings dialog box in the Windows XP Setup Wizard. Also check to make sure your network settings are correct.

Insufficient disk space	Create a new partition using existing free space on the hard disk, delete or create partitions as needed or reformat an existing partition to free up space.
Media errors	Maybe the CD-ROM you are installing from is dirty or damaged. Try using a different CD or trying the affected CD in a different machine.
Nonsupported CD drive	Swap out the drive for a supported drive or try a network install instead. (KB# Q228852)

Log files created during Setup

Logfile name	Description
setupact.log	Action Log – records setup actions in a chronological order. Includes copied files and registry entries as well as entries made to the error log.
Setuperr.log	Error Log – records all errors that occur during setup and includes severity of error. Log viewer shows error log at end of setup if errors occur.
Comsetup.log	Used for Optional Component manager and COM+ components.
Setupapi.log	Logs entries each time a line from an .INF file is implemented. Indicates failures in .INF file implementations.
Netsetup.log	Records activity for joining a domain or workgroup.
Mmdet.log	Records detection of multimedia devices, their port ranges, etc.

Implementing and Conducting Administration of Resources

Understanding FAT and NTFS File Systems

- NTFS provides optimum security and reliability through its ability to lock down individual files and folders on a user-by-user basis. Advanced features such as disk compression, disk quotas and encryption make it the file system recommended by 9 out of 10 MCSEs. (KB# Q244600)
- FAT and FAT32 are only used for dual-booting between Windows XP and another operating system (like DOS 6.22, Win 3.1 or Win 95/98). (KB# Q184006)
- Existing NT 4.0 NTFS system partitions will be upgraded to Windows XP NTFS automatically. If you wish to dual-boot between NT4.0, Windows 2000, or Windows XP you must first install Service Pack 4 on the NT4.0 machine. This will allow it to read the upgraded NTFS partitions, but advanced features such as EFS and Disk Quotas will be disabled. (KB# Q197056 & Q184299)
- Use **convert.exe** to convert a FAT or FAT32 file system to NTFS. NTFS partitions cannot be converted to FAT or FAT32 - the partition must be deleted and recreated as FAT or FAT32 (KB# Q156560 & Q214579)
- You cannot convert a FAT partition to FAT32 using **convert.exe**. (KB# Q197627)

NTFS file and folder permissions: (KB#S Q183090, Q244600)

File attributes when copying/moving within a partition or between partitions:

Copying within a partition	Creates a new file resembling the old file. Inherits the target folder's permissions.
Moving within a partition	Does not create a new file. Simply updates directory pointers. File keeps its original permissions.
Moving across partitions	Creates a new file resembling the old file, and deletes the old file. Inherits the target folders permissions.

Miscellaneous:

- NTFS in Windows 2000 and Windows XP Professional features enhancements not found in Windows NT 4.0 version 4: Reparse Points, Encrypting File System (EFS), Disk Quotas, Volume Mount Points, SID Searching, Bulk ACL Checking, and Sparse File Support. (KB# Q183090)
- Volume Mount Points allow new volumes to be added to the file system without needing to assign a drive letter to it. Instead of mounting a CD-ROM as drive E:, it can be mounted and accessed under an existing drive (e.g., C:\CD-ROM).
- Sparse File Support prevents files containing large consecutive areas of zero bits from being allocated corresponding physical space on the drive and improves system performance.
- NTFS partitions can be de-fragmented in Windows XP (as can FAT and FAT32 partitions). Use **Start > Programs > Accessories > System Tools > Disk Defragmenter**.
- Local security access can be set on a NTFS volume.
- Files moved from an NTFS partition to a FAT partition do not retain their attributes or security descriptors, but will retain their long filenames.
- Permissions are cumulative, except for Deny, which overrides anything.
- File permissions override the permissions of its parent folder.
- Anytime a new file is created, the file will inherit permissions from the target folder.
- The **cacls.exe** utility is used to modify NTFS volume permissions. (KB# Q237701)
- Windows XP supports disk-based quotas. Quotas can be set on NTFS volumes, but not on FAT or FAT32 volumes. Quotas cannot be set on individual folders within a NTFS partition. Quotas can be set on both Basic and Dynamic disks. (KB# Q183322)
- Disk information is stored on the physical disk itself, facilitating moving hard drives between systems. As managing disk numbering can become quite complex, the **dmdiag.exe** utility has been provided. (KB# Q222470)

- If you accidentally start an NTFS conversion on the wrong FAT or FAT32 volume, you still have a chance to cancel it before restarting your system. Go into the registry and change the following key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager and change the *BootExecute* entry to: **autocheck autochk *** (KB# Q130913)

Basic and Dynamic Storage: (KB# Q222189)

Windows XP supports both *Basic* and *Dynamic* storage. In basic storage you divide a hard disk into partitions. Windows XP recognizes primary and extended partitions. A disk initialized for basic storage is called a *Basic disk.* It can contain primary partitions, extended partitions and logical drives. Basic volumes cannot be created on dynamic disks. Basic volumes should be used when dual-booting between Windows XP and DOS, Windows 3.x, Windows 95/98 and all version of Windows NT. (KB# Q175761)

Dynamic storage (Windows 2000 and Windows XP only) allows you to create a single partition that includes the entire hard disk. A disk initialized for dynamic storage is called a *Dynamic disk.* Dynamic disks are divided into volumes that can include portions of one, or many, disks. These can be resized without needing to restart the operating system. (KB# Q225551)

While both Windows 2000 and Windows XP can both read Dynamic Disks, you should not use them in a dual-boot scenario between the two operating systems. Only one of the operating systems can "own" the set of Dynamic Disks. Never use Dynamic disks in any dual-boot scenario.

Translation of terms between Basic and Dynamic Disks

Basic Disks	Dynamic Disks
Active partition	Active volume
Extended partition	Volume and unallocated space
Logical drive	Simple volume
Mirror set	Mirrored volume (Server only)
Primary partition	Simple volume
Stripe set	Striped volume
Stripe set with parity	RAID-5 volume (Server only)
System and boot partitions	System and boot volumes
Volume set	Spanned volumes

There are three Dynamic Volume types

Simple volume - contains space from a single disk.

Spanned volume - contains space from multiple disks (maximum of 32). Data storage first fills one volume before going to the next. If a volume in a spanned set fails, all data in the spanned volume set is lost. Performance is degraded as disks in spanned volume sets are read sequentially.

Striped set - contains free space from multiple disks (maximum of 32) in one logical drive. Increases performance by reading/writing data from all disks at the same rate. If a disk in a stripe set fails, all data is lost.

Dynamic Volume States

State	Description
Failed	Volume cannot be automatically restarted and needs to be repaired
Healthy	Is accessible and has no known problems
Healthy (at risk)	Accessible, but I/O errors have been detected on the disk. Underlying disk is displayed as Online (Errors)
Initializing	Volume is being initialized and will be displayed as healthy when process is complete

Miscellaneous

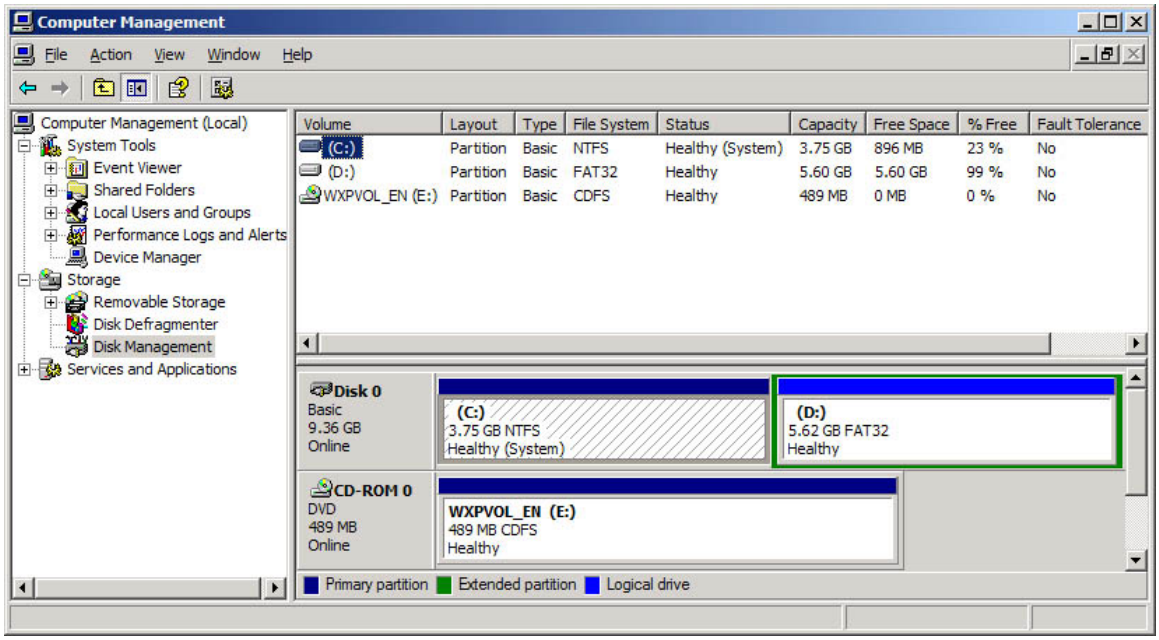
- Cannot be directly accessed by DOS, Win95/98 or any versions of Windows NT if you are dual-booting, as they do not use the traditional disk organization scheme of partitions and logical volumes.

- The MBR on dynamic disks contains a pointer to disk configuration data stored in the last 1 MB of space at the end of the disk. (KB# Q197738)
- Dynamic volumes that were upgraded from basic disk partitions cannot be extended, especially the system volume that holds hardware-specific files required to start Windows XP and the boot volume. Volumes created after the disk was upgraded to dynamic can be extended. (KB# Q222188)
- When installing Windows XP, if a dynamic volume is created from unallocated space on a dynamic disk, Windows XP cannot be installed on that volume. (KB# Q216341)
- Not supported on portable computers or removable media. (KB# Q232463)
- The disk sector size must be 512 bytes to convert a Basic Disk to Dynamic. Use the **chkdsk** command to make sure your disk has the right sized sectors.
- A boot disk that has been converted from Basic to Dynamic cannot be converted back to basic. (KB# Q217226)
- There is NO fault-tolerance with Windows XP Professional. Fault-tolerance (RAID levels 1 and 5) is only available in Windows 2000 and the upcoming Windows .NET Server families. (KB# Q113932)

When using the Disk Management Snap-in Tool

- Whenever you add a new disk in a computer it is added as Basic Storage (shown in Figure 3)
- To manage disks on a remote computer you must create a custom console focused on another computer. Choose **Start** > **Run** and type **mmc**. Press **Enter**. On console menu click Add/Remove Snap-in. Click Add. Click Disk Management then click Add. When Choose Computer dialog box appears choose the remote system.
- Every time you remove or add a new disk to your computer you must choose Rescan Disks.
- Dynamic Disks that have been removed from another computer will appear labeled as Foreign. Choose "Import Foreign Disk" and a wizard appears to provide instructions.
- For multiple Dynamic Disks removed from another computer, they will appear as a group. Right-click on any of the disks and choose "Add Disk".
- Disks can be upgraded from Basic to Dynamic storage at any time but must contain at least 1 MB of unallocated space for the upgrade to work.

Figure 3 – Disk Management



Using Diskpart.exe

Diskpart is a new command-line tool that duplicates most of the functionality of the GUI Disk Management MMC snap-in. Because **diskpart** is a command-line tool, its operation can be scripted making it enormously powerful.
When you first start **diskpart** you must select the disk you are using by its object number. For example:
Diskpart
select disk 0
assign letter c
…selects the first fixed disk in my system and assigns it the drive letter C. All commands I give to **diskpart** now will be performed on this disk until I select another disk. Here is the syntax of a **diskpart** command:
diskpart [**/add** | **/delete**] [*device_name* | *drive_name* | *partition_name*] [*size*]
You cannot format disks using **diskpart** – you must do this using the **format** command from the command line.
A complete list of **diskpart** commands can be found in the *deploy.chm* file that is included in DEPLOY.CAB on the XP product CD.

Windows File Protection Feature (WFP): (KB# Q222193)

- Introduced in Windows 2000, this feature has been carried over to Windows XP. It prevents the replacement of certain monitored system files (important DLLs and EXEs in the %systemroot%\system32 directory).
- Uses file signatures and code signing to verify if protected system files are the Microsoft versions.
- WFP does not generate signatures of any type.
- Critical DLLs are restored from the %systemroot%\system32\dllcache directory. Default maximum size for Professional is 50MB. Editing the Registry can increase this. (KB# Q229656)

Local and network print devices

- Windows XP Professional supports the following printer ports: Line Printer (LPT), COM, USB, IEEE 1394, and network attached devices.
- Print services can only be provided for Windows and UNIX clients on Windows XP Professional. (KB# Q124734)
- You can install print drivers for the following operating systems: Windows XP, Win2000, WinNT 4, WinNT 3.51 and Windows 95/98. (KB# Q142667 explains how to set up print drivers for Windows 95.) The print drivers for the various operating systems are automatically downloaded to the client the first time it connects, if the drivers are present. The NT, 2000, and XP clients automatically check for newer versions of the drivers. Windows 9x clients do not automatically check for newer versions.
- Internet Printing is a feature found in both Windows 2000 and Windows XP. You have the option of entering the URL where your printer is located. The print server must be a Windows XP Server running Internet Information Server or a Windows XP Professional system running Personal Web Server - all shared printers can be viewed at: http://*servername*/printers.
- Print Pooling allows two or more identical printers to be installed as one logical printer.
- Print Priority is set by creating multiple logical printers for one physical printer and assigning different priorities to each. Priority ranges from 1, the lowest (default) to 99, the highest.
- Enabling "Availability" option allows the Administrator to specify the hours the printer is available.
- Use Separator Pages to separate print jobs at a shared printer. A template for the separator page can be created and saved in the %systemroot%\system32 directory with a .SEP file extension. (KB# Q102712)
- You can select Restart in the printer's menu to reprint a document. This is useful when a document is printing and the printer jams. Resume can be selected to start printing where you left off.

- You can change the directory containing the print spooler in the advanced server properties for the printer. (KB# Q123747)
- To remedy a stalled spooler, you will need to stop and restart the spooler services in the Services applet in Administrative Tools in the Control Panel. (KB# Q240683)
- Use the **fixprnsv.exe** command-line utility to resolve printer incompatibility issues. (KB# Q247196)

Implementing, Managing, and Troubleshooting Hardware Devices and Drivers: (KB# Q199276)

Miscellaneous

- Windows XP fully supports the Plug and Play (PnP) standard. (KB# Q133159)
- Use the "System Information" snap-in to *view* configuration information about your computer (or create a custom console focused on another computer - powerful tool!!).
- "Hardware Resources" under System Information allow you to view Conflicts/Sharing, DMAs, IRQs, Forced Hardware, I/O and Memory.
- Hardware is added and removed using the "Add/Remove Hardware" applet in the Control Panel (can also be accessed from **Control Panel > System > Hardware > Hardware Wizard**).
- All currently installed hardware is managed through the "Device Manager" snap-in.
- To troubleshoot a device using Device Manager, click the "Troubleshoot" button on the General tab.

Disk devices

- Managed through "Computer Management" under **Control Panel > Administrative tools** or by creating a custom console and adding the "Disk Management" snap-in. Choosing the "Computer Management" snap-in for your custom console gives you the following tools: Disk Management, Disk Defragmenter, Logical Drives and Removable Storage. There is a separate snap-in for each of these tools except for Logical Drives.
- Using Disk Management, you can create, delete, and format partitions as FAT, FAT32 and NTFS. Can also be used to change volume labels, reassign drive letters, check drives for errors, and backup drives.
- Defragment drives by using "Disk Defragmenter" under "Computer Management" or add the "Disk Defragmenter" snap-in to your own custom console. (KB# Q227463)
- Removable media are managed through the "Removable Media" snap-in.

Display devices

- Desktop display properties (software settings) are managed through the Display applet in Control Panel.
- Display adapters are installed, removed and have their drivers updated through "Display Adapters" under the Device Manager.
- Monitors are installed, removed, and have their drivers updated through "Monitors" under the Device Manager.
- Windows XP Professional supports multiple monitors running concurrently.

Mobile computers

Hardware

- PCMCIA (PC Card) adapters, USB ports, IEEE 1394 (FireWire), and Infrared devices are supported. These are managed through Device Manager.
- Hot (computer is fully powered) and warm (computer is in suspend mode) docking and undocking are now fully supported for computers with a PnP BIOS.
- Support is provided for Advanced Power Management (APM) and Advanced Configuration and Power Interface (ACPI). (KB# Q242495)
- Hibernation (complete power down while maintaining state of open programs and connected hardware) and Standby (deep sleep with some power) modes are supported, extending battery life.
- When a PC Card, USB or Infrared device is installed, Windows XP will automatically recognize and configure it (if it meets PnP specifications). If Windows does not have an entry in its driver base for the new hardware, you will be prompted to supply one.
- Equipping mobile computers with SmartCards and Encrypting File System decreases the likelihood of confidential corporate data being compromised if the computer is stolen or lost.
- Use hardware profiles for mobile computers. Accessed through **Control Panel > System applet > Hardware tab > Hardware Profiles**. Multiple profiles can be created and designated as a docked or undocked portable computer.

Power Management

The Power Management features built into Windows XP Professional are designed to help portable computer users extend their battery life (a major worry when you're using your system in a place with no plug-ins available).

Power Schemes

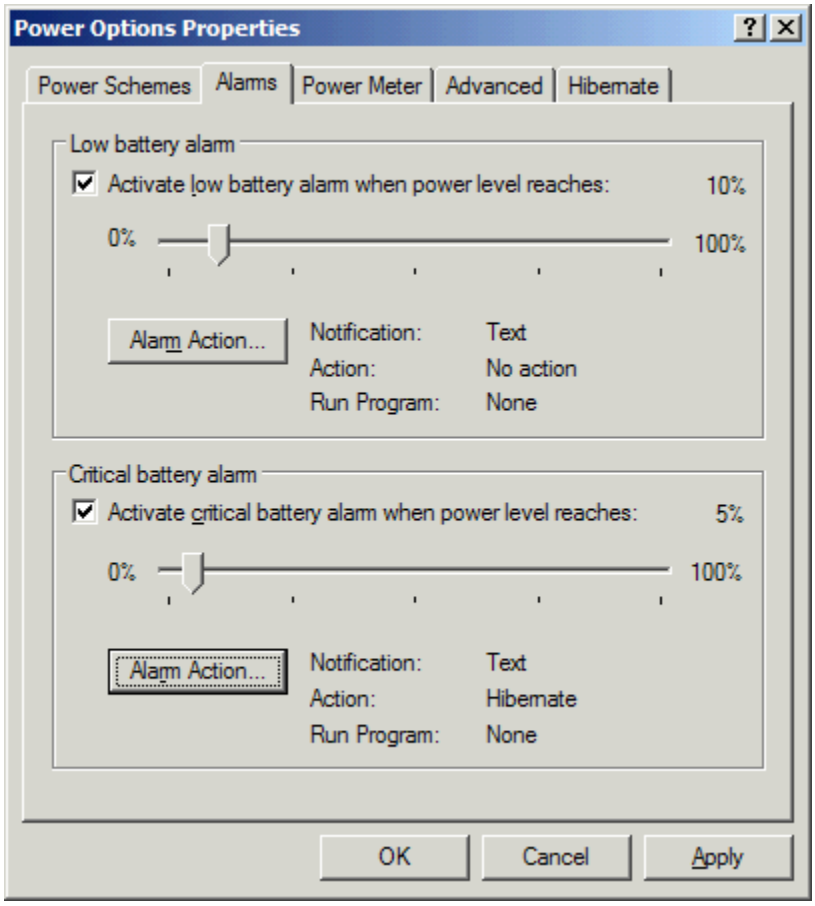
Scheme name	What it does
Always On	Constant power to the system maintained while plugged in or while running on batteries.
Home Office/Desk	Constant power to the system maintained while plugged in.
Max Battery	Constant power to the system maintained while plugged in, but system will start powering down within one minute of inactivity when on battery power.
Minimal Power Management	Constant power to the system maintained while plugged in, but system starts to power down within 3 to 15 minutes when on battery.
Portable/Laptop	Everything shuts down with between 5 – 30 minutes when plugged in, faster if running on batteries.
Presentation	Monitor always on whether unit is plugged in or running on batteries. Rest of the system kept active while plugged in.

Alarms

There are two types of low battery alarms that can be set (shown in Figure 4). You can configure each alarm to simply pop up a dialog warning of the low battery state, run a program, or perform an action:

1. Low battery alarm – this is the "hey, your batteries are getting low you might want to wrap things up" alarm. You hear this alarm first.
2. Critical battery alarm – if you haven't shut down your system yet and reach the second pre-defined threshold, your computer can warn you again or go into hibernation if necessary.

Figure 4 – Alarm Settings



Advanced Settings

- *Standby* – this is a low power state where your computer runs using minimal power. Portable computers that support APM can go into standby mode. Your desktop state is not saved in standby mode.
- *Hibernate* – when your computer goes into hibernation the contents of its memory and desktop state are written to the hard drive. The computer is then completely powered down. The next time the computer is started the hibernation information is pulled from disk back into memory and your desktop state is restored (requires ACPI).

Input and output (I/O) devices

- Keyboards are installed under "Keyboards" in Device Manager.
- Mice, graphics tablets and other pointing devices are installed under "Mice and other pointing devices" in Device Manager.
- Troubleshoot I/O resource conflicts using the "System Information" snap-in. Look under **Hardware Resources > I/O** for a list of memory ranges in use.

Updating drivers

- Drivers are updated using Device Manager. Highlight the device, right-click and choose Properties. A properties dialog appears. Choose the Drivers tab and then the Update Driver... button.
- Microsoft recommends using Microsoft digitally signed drivers whenever possible. Digitally signed drivers are certified by Microsoft to have met standards set by the Windows Hardware Quality Lab. (KB# Q244617)
- The Driver.cab cabinet file on the Windows XP CD contains all of the drivers the OS ships with. Whenever a driver is updated, WINXP looks here first. The location of this file is stored in a registry key and can be changed: HKLM\Software\Windows\CurrentVersion\Setup\DriverCachePath. (KB# Q230644)
- Only digitally signed drivers are included on the Windows XP product CD or made available from the Windows Update site.
- The Driver Verifier is used to troubleshoot and isolate driver problems. It must be enabled through changing a Registry setting. The Driver Verifier Manager, **verifier.exe**, provides a command-line interface for working with Driver Verifier. (KB# Q244617)

Driver signing: (KB# Q224404)

Configuring Driver Signing: (KB# Q236029)

- Open System applet in Control Panel and click Hardware tab. Then in the Device Manager box, click Driver Signing to display options:
    - ***Ignore*** - Install all files, regardless of file signature
    - ***Warn***- Display a message before installing an unsigned file (default setting)
    - ***Block***- Prevent installation of unsigned files
- The *Apply Setting As System Default* checkbox is only accessible to Administrators

Using System File Checker (sfc.exe): (KB# Q222471)

- ***/scannow*** - scans all protected system files immediately
- ***/scanonce*** - scans all protected system files at next startup
- ***/scanboot***- scans all protected system files at every restart
- ***/cancel***- cancels all pending scans
- ***/quiet*** - replaces incorrect files without prompting
- ***/enable*** - sets Windows File Protection back to defaults
- ***/purgecache*** - purges file cache and forces immediate rescan
- ***/cachesize=x***- sets file cache size

Windows Signature Verification (sigverif.exe)

- running **sigverif** launches File Signature Verification
- checks system files by default, but non-system files can also be checked
- saves search results to Sigverif.txt

Rolling back drivers

Driver rollback is a feature that lets you revert to an older copy of a driver that worked when an upgrade to a new driver goes sour. Here are the points to know for the exam:

- Rollbacks are only possible when there is an existing copy of an older driver.
- Driver rollback is available for all devices except printers, which are controlled through the Printers and Faxes applet, not Device Manager.
- Copies of old drivers are stored in the systemroot%\system32\reinstallbackups\ folder. This folder is automatically created the first time a user updates a driver on their Windows XP system.
- Stored drivers consist of the .SYS files (system configuration) and .INF file (device information file).

Resolving hardware conflicts

- Whenever possible, it is preferable to let Windows attempt to resolve resource conflicts.
- Windows is capable of sharing some resources such as IRQs amongst several different devices. If you assign a resource manually you dedicate it to a particular device and prevent Windows from sharing it with other devices as needed. This can make your resource shortage even worse.
- Never use the Registry Editor to reassign resources unless you have no alternative.

Managing/configuring multiple CPUs

- Adding a processor to your system to improve performance is called scaling. It's typically done for CPU intensive applications such as CAD and graphics rendering.
- Windows XP Professional supports a maximum of two CPUs.
- Windows XP supports Symmetric Multiprocessing (SMP). Processor affinity is also supported. Asymmetric Multiprocessing (ASMP) is not supported.
- Upgrading to multiple CPUs might increase the load on other system resources.
- Update your Windows driver to convert your system from a single to multiple CPUs. This is done through **Device Manager > Computer > Update Driver**. (KB# Q234558)

Install and manage network adapters

- Adapters are installed using the Add/Remove Hardware applet in Control Panel.
- Change the binding order of protocols and the Provider order using Advanced Settings under the Advanced menu of the Network and Dial-up Connections window (accessed by right-clicking on My Network Places icon).
- Each network adapter has an icon in Network and Dial-up connection. Right click on the icon to set its properties, install protocols, change addresses, etc.

Troubleshooting the boot process

Files used in the Windows XP boot process: (KB# Q114841)

File:	Location:
Ntldr	System partition root
Boot.ini	System partition root (KB# Q99743)
Bootsect.dos	System partition root
Ntdetect.com	System partition root
Ntbootdd.sys*	System partition root
Ntoskrnl.exe	%systemroot%\System32
Hal.dll	%systemroot%\System32
System	%systemroot%\System32\Config

* Optional - only if system partition is on SCSI disk with BIOS disabled.

ARC paths in BOOT.INI: (KB# Q113977 & Q119467)

The Advanced Risc Computing (ARC) path is located in the BOOT.INI and is used by NTLDR to determine which disk contains the operating system. (KB# Q102873)

multi(x)	Specifies SCSI controller with the BIOS enabled, or non-SCSI controller. x=ordinal number of controller.
scsi(x)	Defines SCSI controller with the BIOS disabled. x=ordinal number of controller.
Disk(x)	Defines SCSI disk that the OS resides on. When *multi* is used, x=0. When *scsi* is used, x= the SCSI ID number of the disk with the OS.
rdisk(x)	Defines disk that the OS resides on. Used when OS does not reside on a SCSI disk. x=0-1 if on primary controller. x=2-3 if on multi-channel EIDE controller.
partition(x)	Specifies partition number that the OS resides on. x=cardinal number of partition, and the lowest possible value is 1.

multi(0)disk(0)rdisk(0)partition(1). These are the lowest numbers that an ARC path can have.

BOOT.INI switches: (KB# Q239780)

- **/basevideo** - boots using standard VGA driver
- /**fastdetect=[com*x,y,z*]** - disables serial mouse detection or all COM ports if port not specified. Included by default
- **/maxmem:*n*** - specifies amount of RAM used - use when a memory chip may be bad
- **/noguiboot** - boots Windows without displaying graphical startup screen
- **/sos** - displays device driver names as they load
- **/bootlog** - enable boot logging
- **/safeboot:minimal** - boot in safe mode
- **/safeboot:minimal(alternateshell)** - safe mode with command prompt
- **/safeboot:network** - safe mode with networking support (KB# Q236346)

Booting in Safe Mode: (KB# Q202485)

- Enter safe mode by pressing F8 during the operating system selection phase
- Safe mode loads basic files/drivers, VGA monitor, keyboard, mouse, mass storage and default system services. Networking is not started in safe mode. (KB# Q199175)
- ***Enable Boot Logging*** - logs loading of drivers and services to ntbtlog.txt in the *windir* folder
- ***Enable VGA Mode*** - boots Windows with VGA driver
- ***Last Known Good Configuration*** - uses registry info from previous boot. Used to recover from botched driver installs and registry changes

- ***Recovery Console*** - only appears if it was installed using **winnt32 /cmdcons** or specified in the unattended setup file
- ***Directory Services Restore Mode*** - only in Server, not applicable to Win2000 Professional
- ***Debugging Mode*** - again, only in Server
- ***Boot Normally*** - lets you boot, uh, normally ;-)

Windows XP Control Sets: (KB# Q142033)

- Found under HKEY_LOCAL_MACHINE\System\Select - has four entries
- ***Current***- CurrentControlSet. Any changes made to the registry modify information in CurrentControlSet
- ***Default*** - control set used next time Windows XP starts. Default and current contain the same control set number
- ***Failed*** - control set marked as failed when the computer was last started using the LastKnownGood control set
- ***LastKnownGood*** - after a successful logon, the Clone control set is copied here

Running the Recovery Console: (KB# Q229716)

- Insert Windows XP CD into drive, change to the i386 folder and run **winnt32 /cmdcons**. (KB# Q216417)
- After it is installed, it can be selected from the "Please Select Operating System to Start" menu.
- When starting Recovery Console, you must log on as Administrator. (KB# Q239803)
- Can also be run from Windows XP Setup, repair option.
- Allows you to boot to a "DOS Prompt" when your file system is formatted with NTFS.
- Looks like DOS, but is very limited. By default, you can copy from removable media to hard disk, but not vice versa - console can't be used to copy files to other media (KB# Q240831). As well, by default, the wildcards in the copy command don't work (KB# Q235364). You can't read or list files on any partition except for system partition.
- Can be used to disable services that prevent Windows from booting properly. (KB# Q244905)

Command	Description
Attrib	changes attributes of selected file or folder
Bootcfg	used add to, edit, or remove items from the boot.ini file
cd or chdir	displays current directory or changes directories
Chkdsk	run CheckDisk
Cls	clears screen
Copy	copies from removable media to system folders on hard disk. No wildcards
del or delete	deletes service or folder
Dir	lists contents of selected directory on system partition only
Disable	disables service or driver
Diskpart	replaces FDISK - creates/deletes partitions
Enable	enables service or driver
Expand	extracts a file from a compressed file – use to extract a driver from a cabinet (.CAB) or compressed file
Fixboot	writes new partition boot sector on system partition
Fixmbr	writes new MBR for partition boot sector
Format	formats selected disk
Help	provides online information about the Recovery Console commands
Listsvc	lists all services on WINXP workstation
Logon	lets you choose which WINXP installation to logon to if you have more than one
Map	displays current drive letter mappings
md or mkdir	creates a directory
more or type	displays contents of text file
net use	connects a network share to a drive letter
rd or rmdir	removes a directory
ren or rename	renames a single file
systemroot	makes current directory system root of drive you're logged into

Startup and Recovery Settings

- Accessed through Control Panel > System applet > Advanced tab > Startup and Recovery
- Memory dumps are always saved with the filename memory.dmp. (KB# Q192463)
- Small memory dump needs 64KB of space. Found in %systemroot%\minidump.
- A paging file must be on the system partition and the pagefile itself at least 1 MB larger than the amount of RAM installed for the Write debugging information option to work.

- Use dumpchk.exe to examine contents of memory.dmp. (KB# Q156280)

Windows Report Tool: (KB# Q188104)

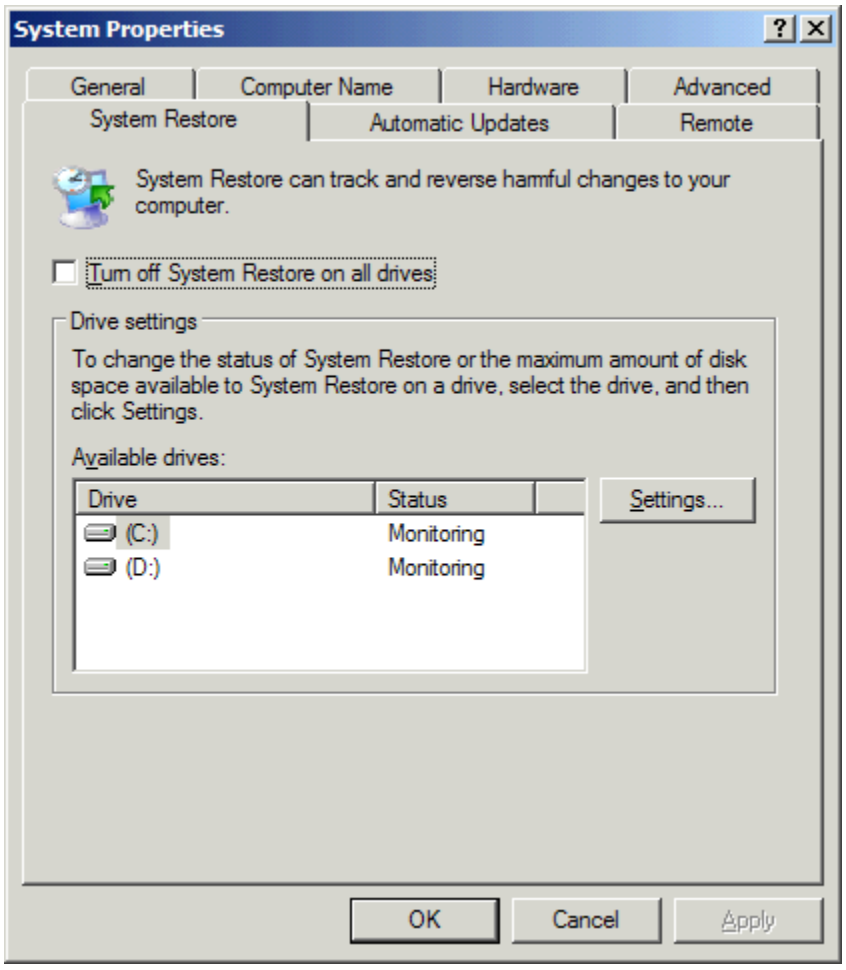
- Used to gather information from your computer to assist support providers in troubleshooting issues. Reports are composed in Windows 98 and Windows XP and then uploaded to a server provided by the support provider using HTTP protocol.
- Reports are stored in a compressed .CAB format and include a Microsoft System Information (.NFO) file.
- The report generated by Windows Report Tool (**winrep.exe**) includes a snapshot of complete system software and hardware settings. Useful for diagnosing software and hardware resource conflicts.

System Restore Points

Enabling System Restore

Windows XP allows you to take snapshots of registry settings and critical system files before you make any major changes to a system. These snapshots are called Restore Points. If something goes wrong during a software installation you can always roll back the system to a pre-installation state by invoking a Restore Point.
Restoring a system rolls back the registry and drivers, and critical system files only – a user's documents are left untouched.
First you need to make sure System Restore is enabled. Right-click on **My Computer**, select **Properties**, and choose the **System Restore** tab from the **Properties** dialog box (shown in Figure 5). The default space allocated from each drive for the System Restore feature is 12%. You can adjust this upwards or downwards depending you're your free drive space situation.
Disabling System Restore deletes all previous Restore Points. A default Restore Point is created the first time System Restore is enabled. Never enable System Restore while in the middle of installing a program or you risk damaging Windows. (KB# Q283081)

Figure 5 – System Restore Dialog



Create a Restore Point

While System Restore can automatically create Restore Points before a program is installed or according to a schedule, you have the option to create Restore Points manually.

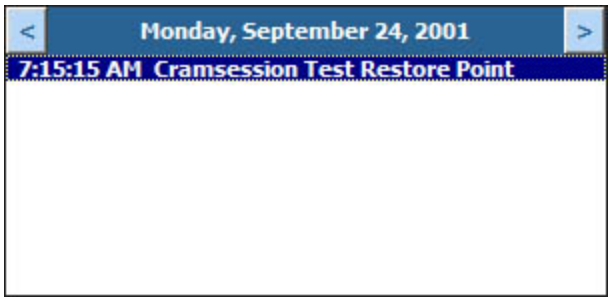
To create a Restore Point, click **Start** > **Programs** > **Accessories** > **System Tools** > **System Restore**. Click the radio button for **Create a Restore Point** and then click **Next**. Enter a name for your Restore Point and then click **Create**. Your Restore Point has just been created.

Rolling back to a Restore Point

To take your system back to a previous Restore Point, click **Start** > **Programs** > **Accessories** > **System Tools** > **System Restore**. Click the radio button for **Restore my computer to an earlier time** and then click **Next**.
You will be presented with two options. You can pick an automatically created Restore Point from the calendar window by selecting a date highlighted in bold (shown in Figure 6) or you can pick a manually created Restore Point from a pick list (shown in Figure 7). Choose a Restore Point and click **Next**. You will be prompted to close all open programs before the restoration takes place. Your computer will reboot and come back up using the restored settings.

Figure 6 – Choosing an automatically created Restore Point

Figure 7 – Choosing a manually created Restore Point



System Restore registry settings

Most of the registry settings for System Restore should be left alone – modifying them could render your Windows operating system inoperable. You can, though, modify the DWORD values we are about to list in this registry key safely:
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore
Here are the DWORD values you can modify:

- *CompressionBurst* – lets you specify the amount of time after a computer sits idle before it starts compressing Restore Point data in the background.
- *DiskPercent* - used for setting the percentage of disk space used for Restore Points. Cannot exceed the DSMax value.
- *DSMax* – specifies the maximum amount of disk space System Restore can use.
- *DSMIN* – if free disk space drops below the value specified here, the System Restore feature becomes inactive.
- *RestoreStatus* – Stores a value indicating whether the last restore operation failed (0), succeeded (1), or was interrupted (2).
- *RPGlobalInterval* – specifies, in seconds, the interval between automatic creation of restore points – default is 24 hours.
- *RPLifeInterval* – specifies, in seconds, the Time To Live (TTL) for Restore Points. When a Restore Point reaches the end of its TTL, it is deleted. Default value is 90 days.
- *RPSessionInterval* – specifies, in seconds, the amount of time System Restore waits before it creates Restore Points while the system is running. Turned off by default (0).
- *ThawInterval* – specifies, in seconds, the amount of time System Restore waits before waking itself from a disabled state.

Automated System Recovery (ASR)

This is a new feature that allows you to create an image of your system partition and write it to a tape backup device or burn it to a CD. Using a special floppy disk called the Automated System Recovery (ASR) Disk, you boot a computer where the operating system has been damaged beyond repair and use the ASR Disk to restore the computer from the image you created.

- Run **ntbackup** and choose the **Automated System Recovery Wizard** from the available options.
- Enter the path and filename for the image file you are creating.
- Insert a blank, formatted 3.5-inch floppy disk into your A: drive then click next.
- The ASR Wizard will create an image file, followed by an ASR floppy disk. The floppy disk contains the ASR state info in the ASR.sif file. Store this file in a safe place along with the image file that you have backed up onto tape or burned onto CD.

Monitoring and Optimizing System Performance and Reliability

Task scheduler: (KB# Q235536 & Q226262)

- Used to automate events such as batch files, scripts and system backups.
- Tasks are stored in the Scheduled Tasks folder in Control Panel.
- Running task with a user name and password allows an account with the required rights to perform the task instead of an administrative account.
- Set security for a task by group or user.

Using offline files

- Offline files replaces My Briefcase and works a lot like Offline Browsing in IE5 and above.
- By default, offline files are stored in the *%systemroot%\CSC* (Client Side Caching) directory.
- Share a folder and set its caching to make it available offline. There are three types of caching:
    - ***manual caching for documents*** - default setting. Users must specify which docs they want available when working offline
    - ***automatic caching for documents*** - all files opened by a user are cached on his local hard disk for offline use - older versions on a user's machine automatically replaced by newer versions from the file share when they exist
    - ***automatic caching for programs*** -same as above, but for programs
- When synchronizing, if you have edited an offline file and another user has also edited the same file, you will be prompted to keep and rename your copy, overwrite your copy with the network version, or to overwrite the network version and lose the other user's changes (a wise SysAdmin will give only a few key people write access to this folder or everyone's work will get messed up).
- Using Synchronization Manager, you can specify which items are synchronized, using which network connection, and when synchronization occurs (at logon, logoff, and when computer is idle).
- The Offline Files feature is not compatible with a feature called Fast User Switching (discussed later).

Performance Console: (KB# Q146005)

- Important objects are *cache* (file system cache used to buffer physical device data), *memory* (physical and virtual/paged memory on system), *physicaldisk* (monitors hard disk as a whole), *logicaldisk* (logical drives, stripe sets and spanned volumes), and *processor* (monitors CPU load).
- *Processor - % Processor Time* counter measures time CPU spends executing a non-idle thread. If it is continually at or above 80%, CPU upgrade is recommended.
- *Processor - Processor Queue Length* - more than 2 threads in queue indicates CPU is a bottleneck for system performance.
- *Processor - % CPU DPC Time* (deferred procedure call) measures software interrupts.
- *Processor - % CPU Interrupts/Sec* measures hardware interrupts. If processor time exceeds 90% and interrupts/time exceeds 15%, check for a poorly written driver (bad drivers can generate excessive interrupts) or else upgrade the CPU.
- *Logical disk - Disk Queue Length* - if averaging more than 2, drive access is a bottleneck. Upgrade disk, hard drive controller, or implement stripe set.
- *Physical disk - Disk Queue Length* - same as above.
- *Physical disk - % Disk Time*- if above 90%, move data/pagefile to another drive or upgrade drive.
- *Memory - Pages/sec* - more than 20 pages per second is a lot of paging - add more RAM.
- *Memory - Committed bytes* - should be less than amount of RAM in computer.
- *diskperf* - physical disk counters are enabled by default, but you will have to type **diskperf -yv** at a command prompt to enable logical disk counters for logical drives or storage volumes. (KB# Q253251)

Performance Alerts and Logs: (KB# Q244640)

- *Alert logs* are like trace logs, but they only log an event, send a message, or run a program when a user-defined threshold has been exceeded
- *Counter logs* record data from local/remote systems on hardware usage and system service activity
- *Trace logs* are event driven and record monitored data such as disk I/O or page faults
- By default, log files are stored in the \Perflogs folder in the system's boot partition
- Save logs in CSV (comma separated value) or TSV (tab separated value) format for import into programs like Excel
- CSV and TSV must be written all at once, they do not support logs that stop and start. Use Binary (.BLG) for logging that is written intermittently
- Logging is used to create a baseline for future reference

Virtual memory/Paging file

- Recommended minimum paging file size is 1.5 times the amount of RAM installed. A system with 64 MB should have a 96 MB page file. Maximum page file size should not exceed 2.5 times the amount of RAM installed.
- Set through **Control Panel > System applet > Advanced tab > Performance Options > Change**.
- The most efficient paging file is spread across several drives, but is not on the system or boot partitions. (KB# Q123747)
- Maximum registry size can also be changed through the Virtual Memory dialog box.

Hardware profiles

- Created to store different sets of configuration settings to meet a user's different needs (usually used with portables) such as whether a computer is docked or undocked.
- User selects the desired profile at Windows XP startup.
- Profiles are created through **Control Panel > System applet > Hardware tab > Hardware Profiles**.
- Devices are enabled and disabled in particular profiles through their properties in the Device Manager snap-in.

Data recovery

- Windows XP Backup is launched through Control Panel > System applet > Backup or by running **ntbackup** from the Start menu. (KB# Q241007)
- Users can back up their own files and files they have read, execute, modify, or full control permission for.
- Users can restore files they have write, modify or full control permission for.
- Administrators and Backup Operators can backup and restore all files regardless of permissions.
- System state information (system registry and COM objects) can be backed up using by selecting **System State** information in **ntbackup** or by using the **systemstate** command from the command line.

Backup type	Description
Normal	All selected files and folders are backed up. Archive attribute is cleared if it exists (fast for restoring)
Copy	All selected files and folders are backed up. Archive attribute is not cleared (fast for restoring)
Incremental	Only selected files and folders that have their archive attribute set are backed up and then

	archive markers are cleared
Differential	Only selected files and folders that have their archive attribute set are backed up but archive attributes are not cleared
Daily	All selected files and folders that have changed throughout the day are backed up. Archive attributes are ignored during the backup and are not cleared afterwards

The Windows XP Registry:

This is a database that stores Windows XP configuration information for all installed software, hardware and users in a hierarchical structure. Consists of five main subtrees:

- ***HKEY_CLASSES_ROOT*** - holds software configuration data, file associations and object linking and embedding (OLE) data
- ***HKEY_CURRENT_CONFIG*** - holds data on active hardware profile extracted from SOFTWARE and SYSTEM hives
- ***HKEY_CURRENT_USER*** - contains data about current user extracted from HKEY_USERS, and additional info pulled down from Windows authentication
- ***HKEY_LOCAL_MACHINE*** - contains all local computer hardware, software, device driver and startup information. Remains constant regardless of the user
- ***HKEY_USERS*** - holds data for user identities and environments, custom settings, etc.

Windows 2000 supported two different registry editing tools:

- The Registry Editor (Regedt32.exe) has a read-only mode, a security menu, and supports the REG_EXPAND_SZ and REG_MULTI_SZ data types as well as the ability to set permissions.
- Regedit.exe does not. Registry Editor automatically saves changes as they are made.

The functionality of both **regedit.exe and regedt32.exe** has been combined into one tool under Windows XP. Typing the name of either executable into the run dialog brings up the same registry editing tool now.

Secondary Logon Service (Run As): (KB# Q225035)

- Similar to the SU (Super User) command in UNIX
- Used to test settings using a particular user account while logged in with a different account
- Select the application icon using a single left-click, hold down the **Shift** key and right-click the icon. When the pop-up menu appears, click **Run As**. This brings up a dialog box titled "Run program as other user" - enter your credentials and click OK

Configuring and Troubleshooting the Desktop Environment

User profiles

A profile is a collection of data and folders that store the user's desktop environment and application settings along with personal data. A profile is automatically created the first time a user logs onto a Windows NT4, Windows 2000, or Windows XP system. Profiles contain the following settings:

- *Accessories* – specific settings for Calculator, HyperTerminal, Notepad, Paint, etc.
- *Application* settings – profile-aware applications, such as Microsoft Word 2000, store user specific configuration information in the user profile.
- *Control Panel* – all custom Control Panel settings are written to the User Profile (e.g., display and mouse settings).
- *Printer Settings* – information on all network printer connections is stored in the user profile. Locally connected printers are not written to the profile.
- *Taskbar Settings* – all taskbar settings.
- *Windows Explorer Settings* – all Explorer settings, as well as persistent connections (mapped drives).

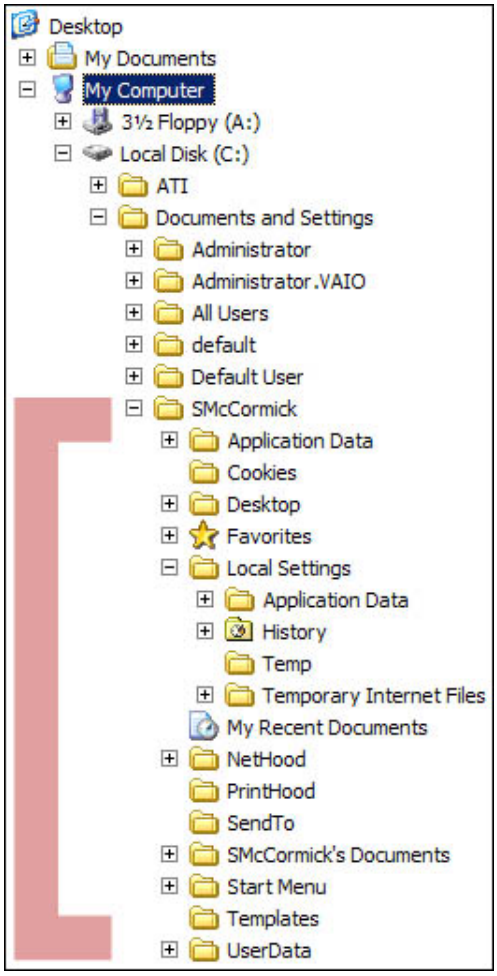
User Profiles also contain the following folders:

- *Application Data* – all profile-aware applications store their information in this folder. Roams with profile by default and can be redirected using Group Policy.
- *Cookies* – all Internet Explorer cookies are stored here. Roams with profile by default.
- *Desktop* – all desktop items including shortcuts and files are stored here. Roams with profile by default and can be redirected using Group Policy.
- *Favorites* – all your Internet Explorer bookmarks go here. Roams with profile by default.
- *Local Settings* – This is where settings that cannot be attached to a roaming profile (discussed later), or that are too large for a Roaming Profile, are stored.
- *%Username% Documents* – this is where all documents created by a user are stored by default. This folder can be redirected to a network server, but this is done separately from Roaming Profiles. Roams with profile by default and can be redirected using Group Policy.
- *NetHood* – where shortcuts to Network Neighborhood items are stored. Roams with profile by default.
- *PrintHood* – where shortcuts to print folder items are stored. Roams with profile by default.
- *Recent* – shortcuts to recently used documents. Roams with profile by default.

- *SendTo* – shortcuts to applications. Roams with profile by default.
- *Start Menu* – shortcuts to program executables. Roams with profile by default and can be redirected using Group Policy.
- *Templates* – shortcuts to template items. Roams with profile by default.

In Windows XP Professional, the default location for User Profiles is the \%systemroot%\Documents and Settings\%username% directory (shown in Figure 8).

Figure 8 – Folder structure of the User Profile



There are three types of User Profiles:

1. *Local User Profile* – Automatically created the first time a user logs onto the computer. Stored on the local hard disk. All changes are stored locally.
2. *Mandatory User Profile* – A profile created for users by Administrators. A user cannot modify the settings in this profile: all changes that the user makes are lost. Kept only for backwards compatibility with NT4 domains – Windows 2000 and newer domains should administer profiles through Group Policy instead.
3. *Roaming User Profile* – This is a User Profile stored on a network server. Users can log on from different machines on the network and still receive the same settings and have access to all of their documents from the network location instead. Roaming profiles are advantageous as they keep the user's state information in a centralized place. Support staff can easily replace a user's computer without losing that user's preferences. All changes made to a Roaming Profile are copied to the network server.

Multiple languages and locations

Changed through the Regional Options applet in Control Panel. Open Region Options and click Input Locale tab to add more locales. Check each locale or language you want your system to support. (KB# Q177561)
On the Regional Options applet General tab, scroll through the items in the box labeled "Your System is Configured to Read and Write Documents in Multiple Languages" to see the available languages, as well as the current default.

Manage and troubleshoot software by using Group Policy

Deploy software by using Group Policy

- Replaces setup.exe. Windows Installer packages are recognized by their .MSI file extension.
- Integrates software installation into Windows XP so that it is now centrally controlled, distributed, and managed from a central-point.
- The software life cycle consists of four phases, *Preparation*, *Deployment*, *Maintenance*, and *Removal*.

Maintain software by using Group Policy

- A software package is installed on a Windows 2000 or Windows .NET Server in a shared directory. A Group Policy Object (GPO) is created. Behavior filters are set in the GPO to determine who gets the software. Then the package is added to the GPO under **User Configuration > Software Settings > Software Installation** (this is done on the server). You are prompted for a publishing method - choose it and say OK.

- Set up Application Categories in **Group Policy > *computer or user config* > Software Settings > Software Installation (right-click) > Properties > Categories > Add**. Creating logical categories helps users locate the software they need under Add/Remove Programs on their client computer. Windows does not ship with any categories by default.
- When upgrading deployed software, AD can either uninstall the old application first or upgrade over top of it.
- When publishing upgrades, they can be optional or mandatory for users but are mandatory when assigned to computers.
- When applications are no longer supported, they can be removed from Software Installation without having to be removed from the systems of users who are using them. They can continue using the software until they remove it themselves, but no one else will be able to install the software through the Start menu, Add/Remove Programs, or by invocation.
- Applications that are no longer used can have their removal forced by an administrator. Software assigned to the user is automatically removed the next time that user logs on. When software is assigned to a computer, it is automatically removed at start up. Users cannot re-install the software.
- Selecting the "Uninstall this application when it falls out of the scope of management" option forces removal of software when a GPO no longer applies.

Configure deployment options

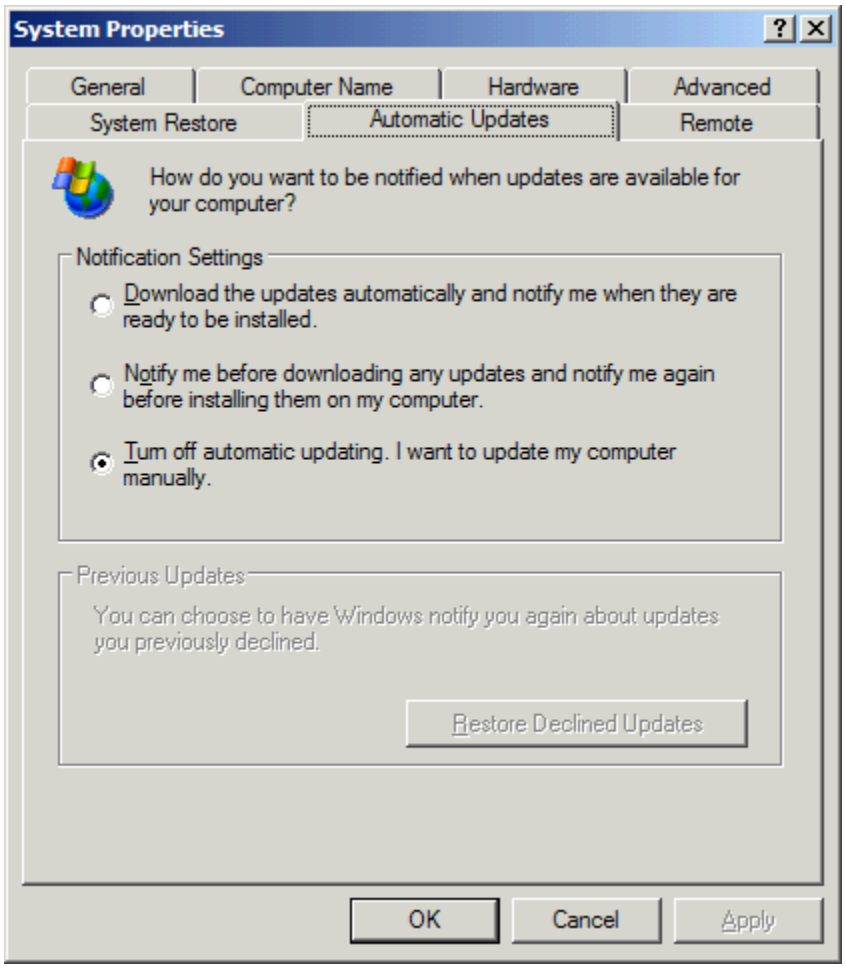
- You can *assign* or *publish* software packages.
- Software that is assigned to a user has a shortcut appear on a user's Start > Programs menu, but is not installed until the first time they use it.
- Software assigned to a computer is installed the next time the computer is started, and before the user can logon.
- When software is assigned to a *user*, the new program is advertised when a user logs on, but is not installed until the user starts the application from an icon or double-clicks a file-type associated with the icon. Software assigned to a *computer* is not advertised - the software is installed automatically. When software is assigned to a computer it can only be removed by a local administrator - users can repair software assigned to computers, but not remove it.
- Published applications are not advertised. They are only installed through Add/Remove Programs in the Control Panel or through *invocation.*
- The software settings of a Group Policy are not refreshed like the rest of the settings. The user may need to logoff/logon or the system may need to be restarted for the new settings to take place (depending on type of software installation).

- Published applications lack resiliency (do not self-repair or re-install if deleted by the user). Finally, applications can only be published to users, not computers.
- With *invocation*, when a user double-clicks on an unknown file type, the client computer queries Active Directory to see what is associated with the file extension. If an application is registered, AD checks to see if it has been published to the user. If it has, it checks for the auto-install permission. If all conditions are met, the application is invoked (installed).
- Non-MSI programs are published as .ZAP files. They cannot take advantage of MSI features such as elevated installation privileges, rolling back an unsuccessful installation, installing on first use of software or feature, etc. (KB# Q231747) .ZAP files can only be published, not assigned.
- Non-MSI programs can be repackaged using a 3rd party tool called WinINSTALL by Veritas software. There is a lite version of this software that was included on the Windows 2000 product CDs that you can use. It lets you take a snapshot of a system, install your application, take another snapshot and create a difference file that becomes your MSI install package. If you wish to assign a non-MSI program to a user or computer, you must first repackage it as an MSI file. (KB# Q236573)
- When software requires a CD key during installation, it can be pushed down with the installer package by typing **misexec /a *<path to .msi file>* PIDKEY="[*CD-Key*]"**. (KB# Q223393)
- Modifications are created using tools provided by the software manufacturer and produce .MST files which tell the Windows Installer what is being modified during the installation. .MST files must be assigned to .MSI packages at the time of deployment. (KB# Q236943)
- Patches are deployed as .MSP files. (KB# Q226936)

Automatic Update

Automatic Update regularly goes online to check with a part of Microsoft's site called Windows Update. Windows Update lets you automatically download and patch your operating system with the latest updates and security patches.
You can change the Automatic Update settings or disable the feature entirely by right-clicking on the **My Computer** icon on your desktop, choosing **Properties**, and then clicking the **Automatic Updates** tab. This brings up the Automatic Updates dialog (shown in Figure 9).

Figure 9 – Automatic Updates Dialog



Configure and troubleshoot desktop settings

Display

- Windows XP Professional supports the connection of up to 10 monitors.
- Portable users can spread their desktop across their notebook monitor in addition to an externally connected monitor using a feature called "Dual View" – works similarly to multiple monitors.
- All monitor settings are configured through the **Display** applet in **Control Panel**.

- The new, brightly-coloured theme that Windows XP comes out of the box with (called "Luna") can best be described as "butt ugly." This is the default theme for clean installations. To prevent your users from going blind you can restore some degree of normalcy by selecting the Windows Classic theme instead that is de rigueur in Windows ME and Windows 2000.

Taskbar

The taskbar now allows grouping of similar items. If you have eight Internet Explorer Web browser windows open they will be grouped into one taskbar item with the number "8" indicating the number of items that are grouped. Clicking on the grouped item brings up a pop-up menu where you can select the specific taskbar item you want to use.

Start Menu

Windows XP includes a new Start Menu that is as useless as it is ugly. The whole point of it is to hide as much of the operating system from the user as possible. You can revert to the older style of Start Menu by right-clicking on the taskbar, selecting **Properties**, and then choosing the **Start Menu** tab. Choosing the **Classic Start Menu** option will take you back to something more palatable.

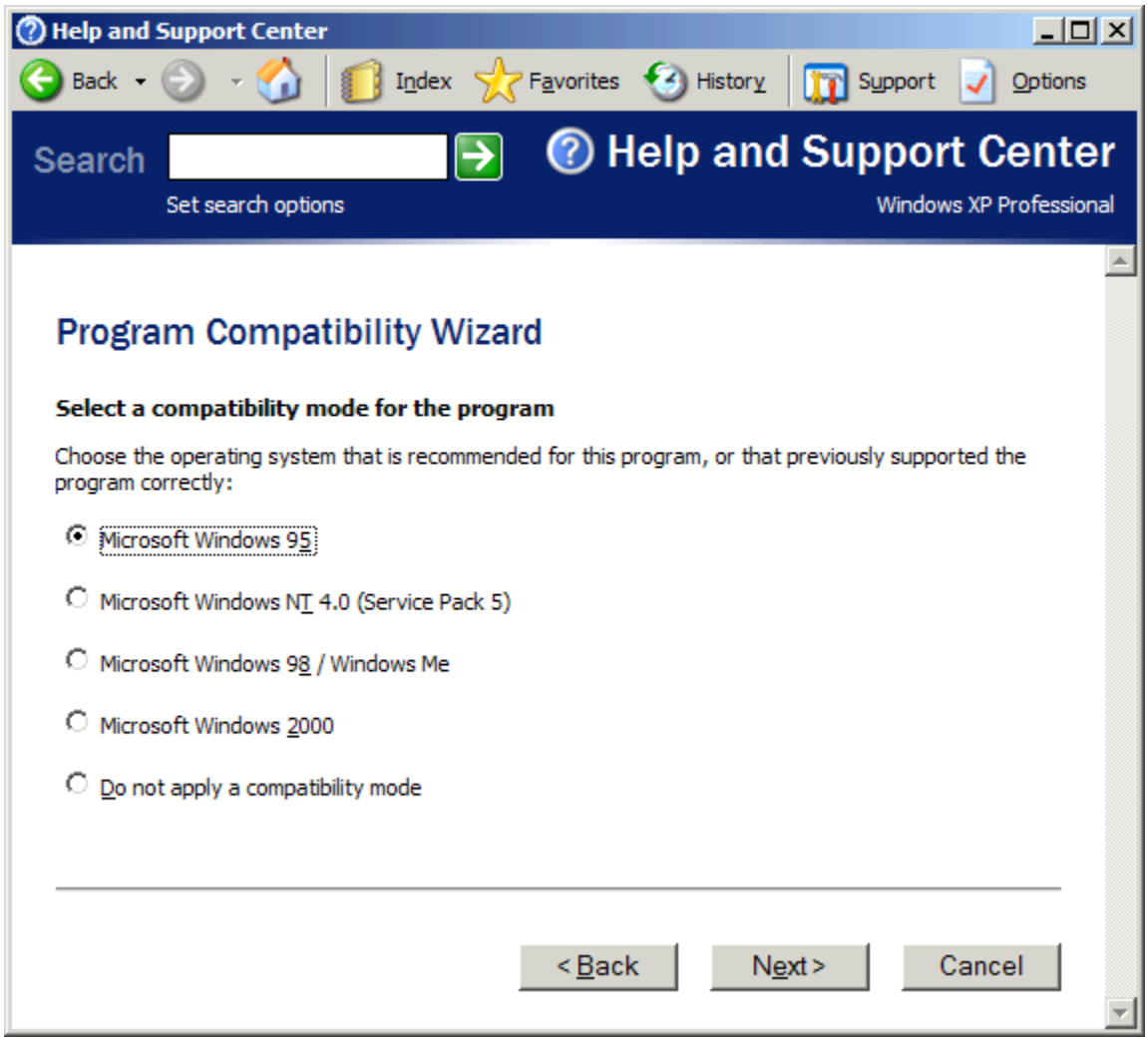
System Tray

Also called the "Notification Area" of the Windows XP taskbar. A new feature in Windows XP allows you to specify which icons appear in the Notification Area. You can have all of your icons showing, or fine-tune things so that you only see icons for active programs while inactive program icons are hidden. This is a very handy feature and helps to reduce the taskbar clutter experienced in previous versions of Windows.

Program Compatibility Wizard (KB# Q301911)

Windows XP includes a new tool designed to provide a compatibility wrapper for programs that were designed for legacy Windows operating systems (mainly Windows 95/98/ME). The Program Compatibility Wizard (PCW) helps trick a program into believing it's being run on an older version of Windows. To launch PCW, click **Start** > **Programs** > **Accessories** > **Program Compatibility Wizard** (shown in Figure 10).

Figure 10 – Program Compatibility Wizard



You can set compatibility for the following operating systems

- Windows 95
- Windows 98/ME
- Windows NT.40 (SP5 or higher)
- Windows 2000

You can choose the following display settings:

- 256 colours
- 640x480 screen resolution
- Disable visual themes (feature that can affect behavior of some programs)

Fax support

- If a fax device (modem) is installed, the Fax applet appears in Control Panel. It does not appear when no fax device installed
- If the Advanced Options tab is not available in the Fax applet, log off then log back on as Administrator
- Use the Fax applet to set up rules for how device receives faxes, number of retries when sending, where to store retrieved and sent faxes, user security permissions, etc.
- The Fax printer in your printer folder cannot be shared

Accessibility services: (KB# Q210894)

- StickyKeys allows you to press multiple key combinations (CTRL-ALT-DEL) one key at a time
- FilterKeys tells the keyboard to ignore brief or repeated keystrokes
- SoundSentry displays visual warnings when your computer makes a sound (for aurally impaired)
- ShowSounds forces programs to display captions for the speech and sounds they make
- MouseKeys lets you control the mouse pointer with the numeric keypad
- Magnifier magnifies a portion of the desktop (for visually impaired) - available during GUI phases of OS installation (KB# Q231843)
- Narrator reads menu options aloud using speech synthesis (for visually impaired) - available during GUI phases of OS installation

Remote Assistance

Overview

This new feature is unique to Windows XP and allows a user to request remote help from a more knowledgeable friend or support technician (in MS terminology, the user providing assistance is referred to as the "expert"). Once the request is accepted, the remote helper can:

- See the user's desktop
- Control the user's desktop (with permission)
- Chat with the user using text or voice
- Send and receive files from the user's system

Remote Assistance is enabled by default in Windows XP. You can enable or disable it by right-clicking on My Computer, dragging to Properties, and then choosing the Remote tab on the System Properties dialog.

Requesting assistance

You can request assistance either from a friend or directly from Microsoft. There are three ways of requesting assistance:

1. Using Windows Messenger
2. By e-mail using a MAPI enabled e-mail client
3. As a file

Important items to remember for the exam:

- Requests must have an expiry set on them. Once the expiry has been reached the helper can no longer respond to the request.
- When using Windows Messenger, requests can be accepted if both parties are behind proxy servers using Network Address Translation (NAT) and have private addresses. When requests are sent by e-mail, NAT between the user and the helper will prevent a Remote Assistance session from taking place.
- Always password protect requests for additional security
- You can view the status of your assistance invitations. Windows XP keeps a record of all invitations you have sent and tells you which are open and which have expired.

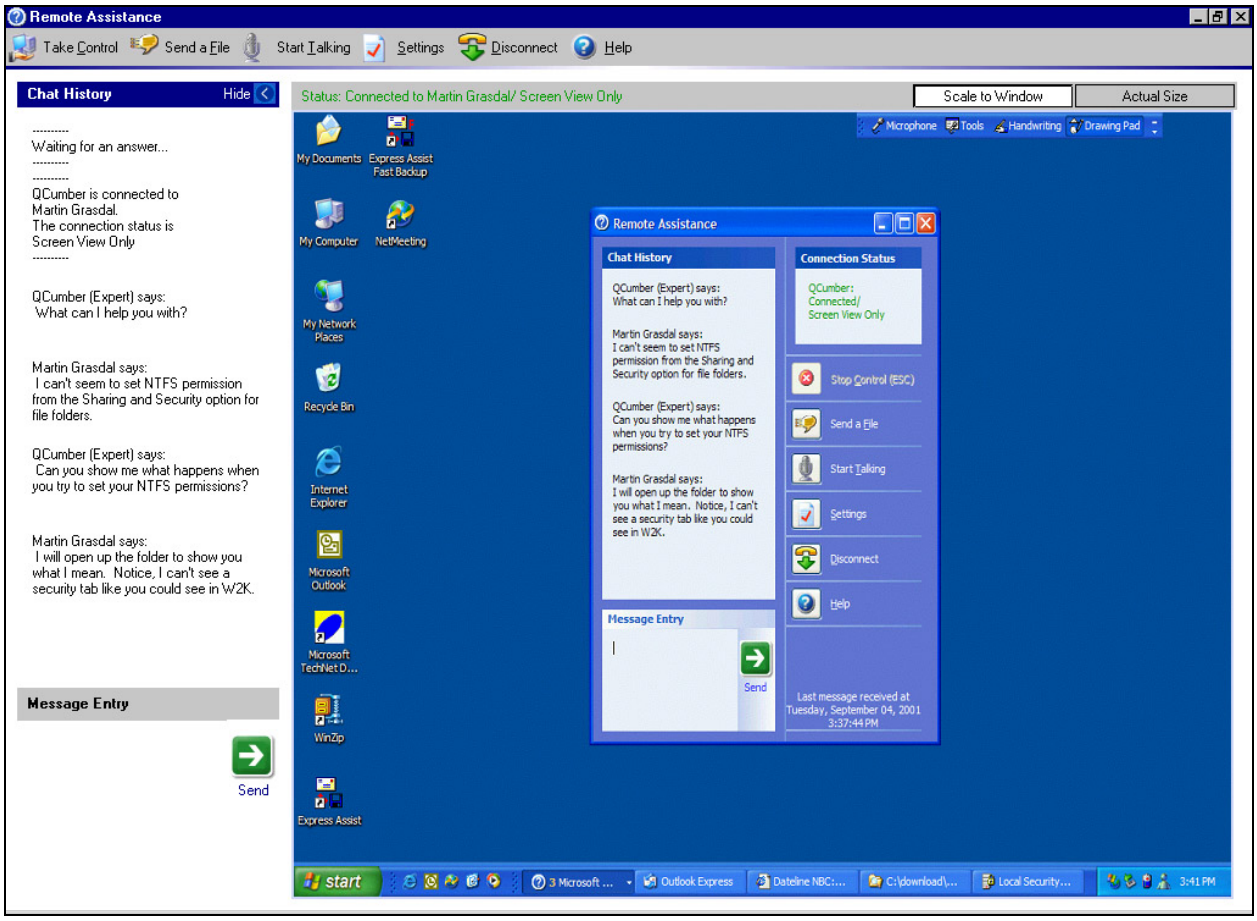
Accepting the request

- If you are using Windows Messenger some text will appear in your chat Window informing you that you have received a Remote Assistance request. Click the hyperlink to Accept the request and Windows XP will connect to the remote system.
- Requests that arrive by e-mail will show up as a plain text e-mail with a file attachment. To begin the Remote Assistance session simply open the file attachment that accompanied the e-mail. The e-mail attachment will have a filename similar to rcbuddyx.MsRIncident (where x is an identifier that may or may not appear).

Remote Assistance Console

Once the helper has connected to the remote system, the Remote Assistance Console will appear (shown in Figure 11).

Figure 11 – Remote Assistance Console



A toolbar with buttons for Remote Assistance helper features appears at the top. The left side of the Window is used for text chat between the two systems. The right-hand pane is used for viewing the remote desktop. You can either view the remote desktop at Actual Size or use Scale to Window to force it to fit your desktop (my preference).
Let's look at the helper's Remote Assistance console first. The following functions are available to you:

- *Take control* – by default, the remote helper can only view a user's desktop. Before the helper can take control of the remote desktop he or she must request control by clicking this button. The remote user must accept your

request before you have control and can take it back at any time by pressing their ESC key.
- *Send a File* – use this feature to send the user an updated driver or file that is needed to repair their system.
- *Start Talking* – this button lets you start a voice chat (Voice Over IP or VOIP) session with the remote user. Both systems will need sound cards, microphones, and speakers/headphones for this to work. Best used over high-bandwidth connections only.
- *Settings* – use this to adjust sound quality and resize your console.
- *Disconnect* – used to end the Remote Assistance session.

Built-in accounts used with Remote Assistance

- *HelpAssistant* – this is the account used by helpers you have invited to provide assistance. It is only ever enabled when there are open assistance invitations. Once all open invitations have expired this account is disabled again.
- *SUPPORT_xxxxxx* – (where xxxxx is a hexadecimal number). This account is only used when assistance is requested directly from Microsoft and it is disabled by default.

Implementing, Managing, and Troubleshooting Network Protocols and Services:

TCP/IP protocol

Miscellaneous

- TCP is an industry-standard suite of protocols
- It is routable and works over most network topologies
- It is the protocol that forms the foundation of the Internet
- It is Installed by default in Windows XP
- Can be used to connect dissimilar systems
- Uses Microsoft Windows Sockets interface (Winsock)
- IP addresses can be entered manually or be provided automatically by a DHCP server
- DNS is used to resolve computer hostnames to IP addresses
- WINS is used to resolve a NetBIOS name to an IP address
- Subnet mask - A value that is used to distinguish the network ID portion of the IP address from the host ID
- Default gateway - A TCP/IP address for the host (typically a router) which you would send packets for routing elsewhere on the network

Automatic Private IP Addressing

Windows 98, Windows ME, Windows 2000 and Windows XP support this feature. When "Obtain An IP Address Automatically" is enabled, but the client cannot obtain an IP address, Automatic Private IP addressing takes over:

- IP address is generated in the form of 169.254.x.y (where x.y is the computer's identifier) and a 16-bit subnet mask (255.255.0.0)
- The computer broadcasts this address to its local subnet
- If no other computer responds to the address, the first system assigns this address to itself
- When using the Auto Private IP, it can only communicate with other computers on the same subnet that also use the 169.254.x.y range with a 16-bit mask
- The 169.254.0.0 - 169.254.255.255 range has been set aside for this purpose by the Internet Assigned Numbers Authority

Alternate TCP/IP Configurations

Windows XP lets you provide an alternate TCP/IP configuration for each network interface in the event the interface is unable to obtain an IP address from a DHCP server. You can choose to use Automatic Private IP Addressing (the default) or to manually specify a configuration instead.

TCP/IP Client Utilities

- Telnet client - Can be used to open a text based console on UNIX, Linux and Windows XP systems (run **telnet *servername***)
- FTP client - Command line based - simple and powerful (run **ftp *servername***)
- Internet Explorer 6 - Microsoft's powerful and thoroughly integrated Web browser
- Outlook Express 6 - SMTP, POP3, IMAP4, NNTP, HTTP, and LDAP complaint E-mail package.

TCP/IP Server Utilities

- Telnet server - Windows XP includes a telnet server service (**net start tlntsvr**) that is limited to a command line text interface and two concurrent users. Set security on your telnet server by running the admin tool, **tlntadmn**. (KB# Q225233)
- Web Server - stripped version of IIS5 Web server. Limited to 10 connections. Must be installed and the service started before sharing your printers using

Web printing or Internet printing. Can be managed using IIS snap-in or Personal Web Manager, a "dumbed-down" GUI for novice users.
- FTP Server - stripped version of Internet Information Server 5 (IIS5) FTP server. Limited to 10 connections but is administered just like the server version using IIS snap-in or the Personal Web Manager.
- FrontPage 2000 Server Extensions - extends the functionality of the Web server and is included in WINXP Pro for developing and testing Web sites before deploying them to a production server.

SMTP Server - does not appear to have limitations on connections but this is most likely because of its integration with LDAP and Active Directory replication. Also works with the form handlers in FrontPage Server Extensions.

Internet Explorer 6

Here are important changes to Internet Explorer 6 to note for the exam:
- The default cipher strength is now 128-bit.
- The Microsoft Virtual Machine for Java is not bundled in with XP thanks to continued legal bickering between MS and Sun Microsystems. The missing component is configured as an "Automatic Download." The first time users attempt to use a java-enabled page that requires the Virtual Machine, they will be prompted to download it from Microsoft's site.
- Internet Explorer now features a Media Toolbar that integrates Windows Media Player into your browser. This new toolbar deftly combines the worst features of both products.
- Microsoft has built a new privacy feature into Internet Explorer based upon the Platform for Privacy Preferences (P3P) standard. By default, all cookies from third-party Web sites that do not contain XML formatted privacy policy information are blocked.

Windows Messenger

MSN Messenger is being re-branded as "Windows Messenger". This is a full featured text chat and videoconferencing client. It is completely integrated into the operating system and plays a pivotal role in Microsoft's Passport/Hailstore/.NET initiative.
Windows Messenger makes use of the Session Initiation Protocol (SIP) support built-into Windows XP. (RFC 2543, 2848, 2976, 3050, 3087)
While Windows Messenger is backwards compatible with your contacts who are using MSN Messenger, the following features will only work between Windows XP Desktops running Windows Messenger:
- Remote Assistance requests
- Videoconferencing

Internet Connection Sharing (ICS)

Internet Connection Sharing is a watered down version of Network Address Translation (NAT) and is intended for small networks, such as those typically found in the home or small business.
Using ICS, one computer, called the ICS host, shares its Internet connection with the rest of the computers on the private network. Other computers on the private network can force the ICS host to initiate a connection to the Internet (if not already active) by beginning a task that requires Internet access, such as starting Internet Explorer or Outlook Express.
The ICS host must have at least one Network Interface Card (NIC) connected to the rest of the private network through a switch or hub and one other network interface that connects to the Internet. This can be either broadband (Cable, DSL, etc.) or a standard dial-up modem.
When ICS is enabled, it will reassign the private adapter the IP address of 192.168.0.1 with a subnet mask of 255.255.255.0. All of the computers inside the private network must be configured to request IP addresses using DHCP. The ICS host will act as its own DHCP and DNS server for the internal private network.
When configuring ICS you can enable the "Internet Discovery and Control" feature. This allows all ICS clients that support Internet Discovery and Control to monitor and manage their ICS connection and even force the ICS server to disconnect from the Internet, if need be. Windows XP clients support Internet Discovery and Control by default. Support for Internet Discovery and Control can be added to Windows 98 or higher clients running IE5 and up by running the Network Setup Wizard (available on the XP product CD) on them.

Internet Connection Firewall (ICF)

Internet Connection Firewall is Microsoft's answer to securing single computers and small networks from the threats inherent today with usage of the Internet. ICF is directly related to Internet Connection Sharing, but the two may be used independently of each other (when used with ICS on the ICS host it can protect your entire network).
ICF is considered a "stateful" firewall—that is to say that it monitors all communications that happen to cross its boundaries and in doing do inspects the source and destination IP address of each message that it sees. To prevent unsolicited traffic from the public (Internet) side of the connection from entering the private side, ICF makes a table that tracks all communications that originate at the ICF computer (in the case of a single computer) or the ICF/ICS host computer (when used in conjunction with ICS) and from all private network computers. All inbound traffic from the Internet is compared against the entries in the table and is only allowed to arrive at the computers in the private network when there is a matching entry in the table showing that the communication exchange began from within the private network.

Communications that originate from a source outside the ICF computer, such as the Internet, are dropped by the firewall unless an entry in the SERVICES tab is made to allow passage. Rather than sending you notifications about activity, ICF silently discards unsolicited communications, stopping common hacking attempts such as port scanning.
When dealing with ICF, there are three important items that you need to understand:

1. To configure ICF, you must be logged on locally as an administrator (or with administrative access). Neither Power Users nor the new security group Network Configuration Operators have the required privileges to modify ICF settings.
2. You should not enable ICF on the network adapter of a machine that does not connect directly to the Internet, as it will interfere with communications between that client and other clients on your network. It is for this reason that the Network Setup Wizard will not allow ICF to be configured on the private connection (the NIC that connects to the internal network) of an ICS configured machine.
3. Certain programs (Outlook 2000 for example) that rely on RPC messages from a server to the client (for new e-mail notification in this case) will not function correctly from behind ICF. This is because the RPC message originates unsolicited from outside the private network (at the ISP's Microsoft Exchange Server in this case). ICF will not be able to find a corresponding entry in its routing table and thus the RPC messages will not be allowed to cross the firewall boundary. The message will be dropped and the user will not be notified of new e-mail. You can send and receive e-mail normally, but you would have to manually check for new e-mail.

To start configuration on ICF: **Start > Settings> Network Connections > Local Area Connection** (as applicable, as you can rename it) **> Properties > Advanced**. Place a check in the check box next to "Protect my computer…". After this is accomplished, click on **Settings**. Doing this opens a new window with three tabs: **Services**, **Security Logging** and **ICMP**.

If your internal network is running any kind of Internet accessible services then the SERVICES tab should definitely get your attention. The default settings allow for none of the available services to be enabled; however you can easily modify this as your situation dictates. If a particular service that you need to support is not listed, you can simply add it.

The **Security Logging** tab deals primarily with what to log, how much to log and where to keep the log. The default settings enable a log located either at C:\WINNT\pfirewall.log (if upgrading from a Windows 2000 Professional or Windows NT 4.0 installation) or C:\WINDOWS\pfirewall.log (if upgrading from Windows 9x/Me

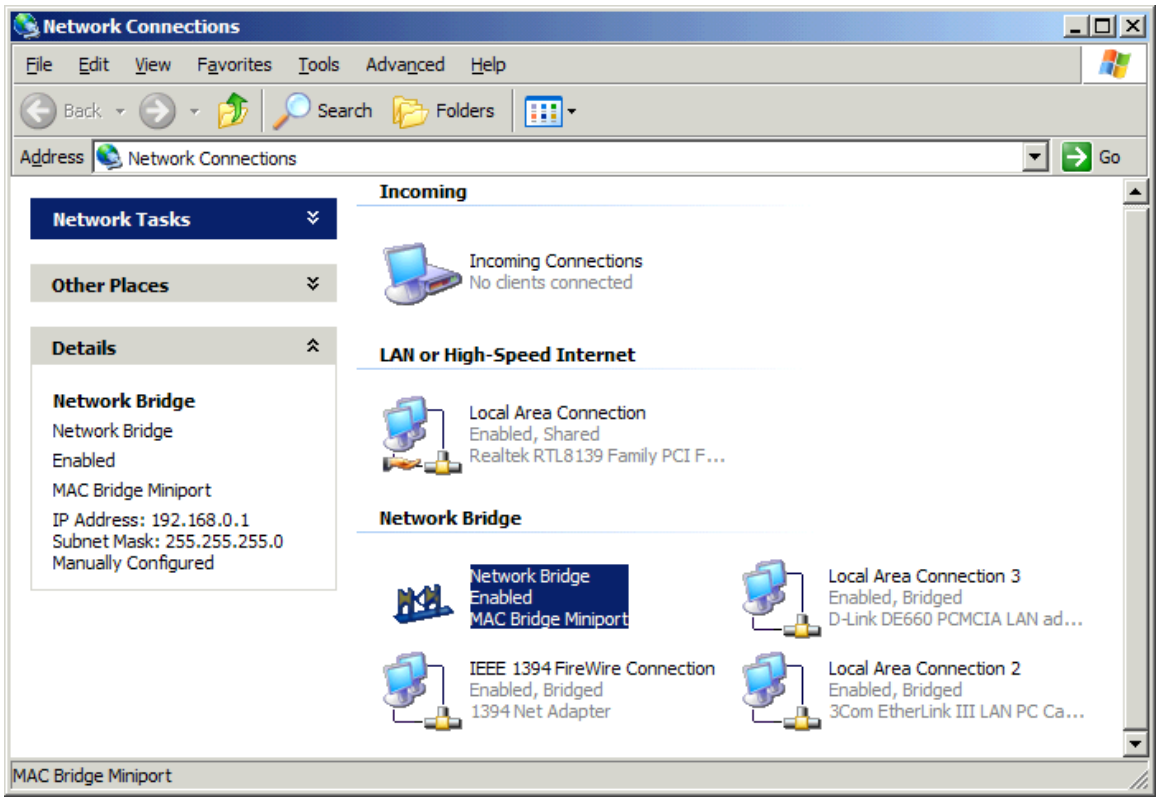
or performing a clean installation). The default log size is 4096KB and can be changed to fit the needs of your situation, though. By default, logging is not in effect.

The last tab is ICMP settings. By default, none of the options are checked. This results in the most secure configuration possible. It may be useful to enable the first option "Allow incoming echo request" as this will enable the use of the PING command against the interface that ICF is configured on.

Network Bridging

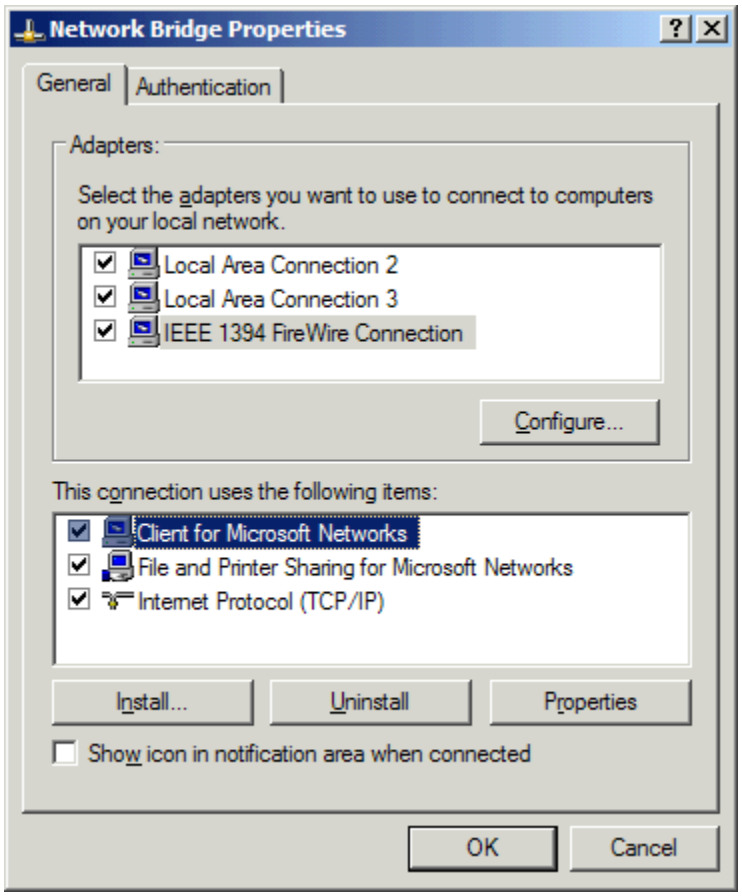
Network Bridging is a new feature in Windows XP that allows you to combine several different network adapters for different networks into a single *bridged* network adapter that behaves as a single network. Bridging takes place at layer two of the OSI Network model, or Data Link layer. Figure 12 shows three network adapters, two Ethernet, and one IEEE 1394 (FireWire) that have been bridged into a single virtual network:

Figure 12 – Network bridging in action



Windows XP treats the bridge as a physically installed device and it is configured in pretty much the same way other installed network devices are, as shown in Figure 13

Figure 13 – Network bridge properties



Remote Desktop Connections

Windows XP Professional ships with a Remote Desktop Connection client installed by default. As well, it includes its own limited version of Terminal Services (called Remote Desktop Connection under Windows XP) that allows users and administrators to remotely work with and administer Windows XP Professional.

Connecting to a remote server

You can access the Remote Desktop Connection client by clicking **Start** > **Programs** > **Accessories** > **Communications** > **Remote Desktop Connections**. This brings up the Remote Connection Dialog box shown in Figure 14:

Figure 14 – Ready to initiate a Remote Desktop Connection

Enter the Computer Name, IP address, or Fully Qualified Domain Name (FQDN) of the computer you wish to connect to and click the **Connect** button. Use the **Options button** to configure some additional parameters for your connection:

- Display settings can include colour depth (if not overridden at the server end) and display size (640x480 to full screen).
- Remote sounds can be redirected to the local system.
- You can choose whether or not to redirect devices on the remote computer such as printer ports, serial ports, and disk drives to your local system.
- Choose a level of user experience that includes connection speed, themes, desktop background, bitmap caching, etc.

Connecting to Windows XP Professional

Here are the important points to know for the exam:

- Windows XP Professional only supports a single Remote Desktop Connection. When a remote user connects to a Windows XP Professional system the desktop on the local console automatically locks. Unlocking the desktop forces the remote session to disconnect immediately.
- Windows 95/98/ME, Windows NT 4, and Windows 2000 systems can remotely connect to a Windows XP Remote Desktop Connection session using either the 32-bit Terminal Services Client that ships with Windows 2000 or by installing the Remote Desktop Connection client that is included on the Windows XP product CD.
- To install the Remote Desktop Connection on an older Windows operating system, insert the Windows XP product CD, choose **Perform additional tasks** from the menu, and then **Set up Remote Desktop Connection**.
- Remote Desktop Connections require that port TCP/IP port 3389 for Remote Desktop Protocol be opened.
- Remote Desktop also supports Remote Desktop Web Connection – this is essentially the same as the Terminal Services Advanced Client available for Windows 2000. Clients require IE4 or higher with a special ActiveX control

installed. The Windows XP system offering Remote Desktop Web Connection will need to be configured with the limited version of IIS5 that is included by default. Also ensure that the Remote Desktop Web Connection files are copied to the \Web\TSWeb directory of the Web server.

Troubleshooting: (KB# Q102908)

- Ipconfig and Ipconfig /all - displays current TCP/IP configuration
- Nbtstat - displays statistics for connections using NetBIOS over TCP/IP
- Netstat - displays statistics and connections for TCP/IP protocol
- Ping - tests connections and verifies configurations
- Tracert - checks a route to a remote system
- Common TCP/IP problems are caused by incorrect subnet masks and gateways
- If an IP address works but a hostname doesn't, check DNS settings

NWLink (IPX/SPX) and NetWare Interoperability

- NWLink (MS's version of the IPX/SPX protocol) is the protocol used by Windows XP to allow Netware systems to access its resources. (KB# Q203051)
- NWLink is all that you need to run in order to allow a Windows XP system to run client/server applications from a NetWare server.
- To allow file and print sharing between NT and a NetWare server, CSNW (Client Services for NetWare) must be installed on the Windows XP system. In a Netware 5 environment, the Microsoft client does not support connection to a Netware Server over TCP/IP. You will have to use IPX/SPX or install the Novell NetWare client. (KB# Q235225)
- Gateway Services for NetWare can be implemented on your Windows 2000 Server to provide a MS client system to access your NetWare server by using the Windows 2000 Server as a gateway. (KB# Q121394)
- Frame types for the NWLink protocol must match the computer that the Windows XP system is trying to connect with. Unmatched frame types will cause connectivity problems between the two systems.
- When NWLink is set to autodetect the frame type, it will only detect one type and will go in this order: 802.2, 802.3, ETHERNET_II and 802.5 (Token Ring).
- Netware 3 servers uses Bindery Emulation (Preferred Server in CSNW). Netware 4.x and higher servers use NDS (Default Tree and Context.)
- There are two ways to change a password on a Netware server - SETPASS.EXE and the Change Password option (from the CTRL-ALT-DEL dialog box). The Change Password option is only available to Netware 4.x and higher servers using NDS.

Other protocols

- DLC is a special-purpose, non-routable protocol used by Windows XP to talk with IBM mainframes, AS400s and Hewlett Packard JetDirect printers.
- The NetBEUI protocol is not installed in Windows XP by default – it can be installed from the \VALUEADD\MSFT\NET\NETBEUI directory on the product CD-ROM.
- Windows XP does not support AppleTalk. If you are upgrading a previous version of Windows with AppleTalk installed, this protocol will be removed during the installation process. (KB# Q305989)

Remote Access Services (RAS)

Authentication protocols

- EAP - Extensible Authentication Protocol. A set of APIs in Windows for developing new security protocols as needed to accommodate new technologies. MD5-CHAP and EAP-TLS are two examples of EAP.
- EAP-TLS - Transport Level Security. Primarily used for digital certificates and smart cards.
- MD5-CHAP - Message Digest 5 Challenge Handshake Authentication Protocol. Encrypts usernames and passwords with an MD5 algorithm.
- RADIUS - Remote Authentication Dial-in User Service. Specification for vendor-independent remote user authentication. Windows XP Professional can act as a RADIUS client only.
- MS-CHAP (v1 and 2) - Microsoft Challenge Handshake Authentication Protocol. Encrypts entire session, not just username and password. v2 is supported in Windows XP, Windows 2000,Windows NT4 and Windows 95/98/ME (with DUN 1.5 upgrade) for VPN connections. MS-CHAP cannot be used with non-Microsoft clients. You must use MS-CHAP authentication for PPTP (see below).
- SPAP - Shiva Password Authentication Protocol. Used by Shiva LAN Rover clients. Encrypts password, but not data.
- CHAP - Challenge Handshake Authentication Protocol - encrypts user names and passwords, but not session data. Works with non-Microsoft clients.
- PAP - Password Authentication Protocol. Sends username and password in clear text.

Virtual Private Networks (VPNs)

- PPTP - Point to Point Tunneling Protocol. Creates an encrypted tunnel through an untrusted network. The encryption is provided by Microsoft Point-to-Point Encryption (MPPE), a Microsoft proprietary protocol and is available at 40-bit or 128-bit levels. MPPE requires the use of MS-CHAP.
- L2TP - Layer Two Tunneling Protocol. Works like PPTP as it creates a tunnel, but it does not provide data encryption. Security is provided by using an encryption technology like IPSec.
- Windows XP Professional supports a single inbound VPN connection.

Feature	PPTP	L2TP
Header compression	No	Yes
Tunnel authentication	No	Yes
Built-in encryption	Yes	No
Transmits over IP-based internetwork	Yes	Yes
Transmits over UDP, Frame Relay, X.25 or ATM	No	Yes

Multilink Support: (KB# Q235610)

- Multilinking allows you to combine two or more modems or ISDN adapters into one logical link with increased bandwidth. (KB# Q233171)
- BAP (Bandwidth Allocation Protocol) and BACP (Bandwidth Allocation Control Protocol) enhance multilinking by dynamically adding or dropping links on demand. Settings are configured through RAS policies. (KB# Q244071)
- Enabled from the PPP tab of a RAS server's Properties dialog box. (KB# Q233151)

Setting Callback Security

- Using callback allows you to have the bill charged to your phone number instead of the number of the user calling in. Also used to increase security.
- For roving users like a sales force, choose "Allow Caller to Set The Callback Number" (less secure).

Dial-up networking

- Microsoft technical documentation generally refers to dial-up networking when describing outbound connections. Inbound connections are usually associated with Remote Access Services (RAS).
- All new connections are added using the "Make New Connection" wizard.

- To create a VPN connection, choose Dial-Up To A Private Network Through The Internet, specify whether you need to establish a connection with an ISP first, enter the host name or IP address of the computer/network you are connecting to, and select whether connection is for yourself or all users.
- Dial-up networking entries can be created for modem connections, LAN connections, direct cable connections and Infrared connections.
- PPP is generally preferred because it supports multiple protocols, encryption, and dynamic assignment of IP addresses (KB# Q124036). SLIP is an older protocol that only supports TCP/IP and is used for dialing into legacy UNIX systems.
- Separate icons under Dial-up networking represent all network connections, inbound and outbound - properties, protocols, addresses and services can be individually configured for each.

Using shared resources on a Microsoft Network

The Administrators and Power Users groups can create shared folders on a Windows XP Professional workstation
Windows XP creates administrative shared folders for administrative reasons. These shares are appended with dollar sign ($) that hides the share from users browsing the computer. The system folder (Admin$), the location of the printer drivers (Print$), and the root of each volume (C$, D$, etc.) are all hidden shared folders.
Shared folder permissions apply only when the folder is accessed via the network. By default, the Everyone group is assigned Full Control for all new shared folders. Share level permissions can be applied to FAT, FAT32 and NTFS file systems.
Windows XP Professional systems support a maximum of 10 simultaneous file sharing connections. If higher capacity is needed, consider upgrading to a Windows Server product.

Security levels for network access to shared folders

Full Control	• Is assigned to the Everyone group by default. • Allows user to take ownership of files and folders. • Users can change file access rights. • Grants user all permissions assigned by the Change and Read levels.
Change	• User can add and create files. • Grants ability to modify files. • User can change the attributes of the file. • User can delete files. • Grants user all permissions assigned by the Read level.
Read	• User can display and open files. • User can display the attributes of the file. • User can execute program files.

The "No Access" permission has not been carried over from Windows NT. You can, however, choose to allow or deny shared folder permissions. If you want to deny complete access to a shared folder for a particular user you would grant the user the deny Full Control permission. Microsoft recommends using the Deny functionality sparingly.
When a resource has both File-Level (NTFS) and Share-Level Securities enabled, you combine the highest two securities (assuming that there is not a "deny") and use the most restrictive of the two.

Implementing, Monitoring, and Troubleshooting Security

Active Directory Overview

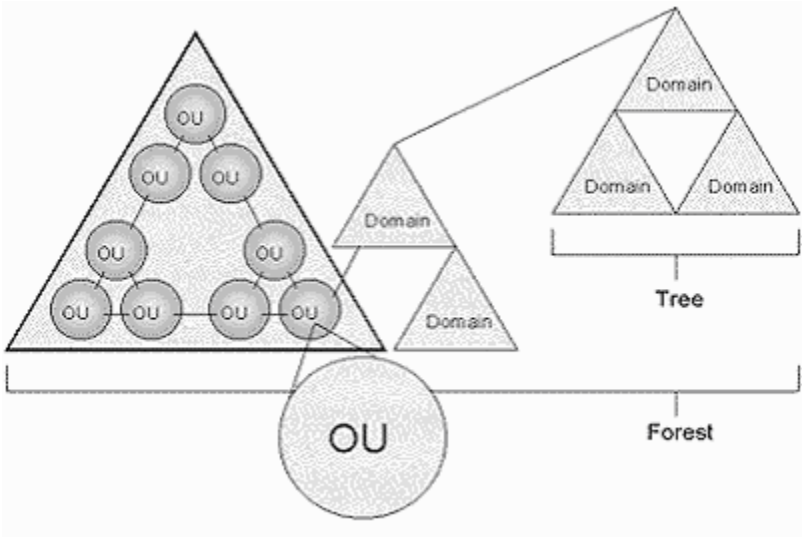
Active Directory (AD) services provide a single point of network management, allowing you to add, remove, and relocate resources easily. It offers significant enhancements over the limitations of the older Windows NT domain based security model. Its features are:

- *Simplified Administration* - AD provides a single point of logon for *all* network resources - an administrator can logon to one computer and administer objects on any computer in the network.
- *Scalability* - NT 4 domains had a practical limitation of about 40,000 objects. AD scales to millions of objects, if needed.

- *Open standards support* - uses DNS as its domain naming and location service so Windows XP domain names are also DNS domain names. Support for LDAP v2 and v3 makes AD interoperable with other directory services that support the same, such as Novell's NDS. HTTP support means that AD can be searched using a Web browser. Kerberos 5 support provides interoperability with other products that use the same authentication mechanism.

Active Directory Structure

Figure 15 – Active Directory Components



- *Object* - distinct named set of attributes that represents a network resource such as a computer or a user account.
- *Classes* - logical groupings of objects such as user accounts, computers, domains or organizational units.
- *Organizational Unit (OU)* - container used to organize objects inside a domain into logical administrative groups such as computers, printers, user accounts, file shares, applications and even other OUs.
- *Domain* - all network objects exist within a domain with each domain storing information only about the objects it contains. A domain is a security boundary - access to objects is controlled by Access Control Lists (ACLs). ACLs contain the permissions associated with objects that control which users or types of users can access them. In Windows XP, all security policies and settings (like Administrative rights) do not cross from one domain to another. The Domain Admin only has the right to set policies within his/her domain. Enterprise Admins can set rights across all domains in a forest.

- *Tree* - a grouping or hierarchical arrangement of one or more Windows XP domains that share a contiguous names space (e.g. crams.cramsession.com, sales.cramsession.com, and questions.cramsession.com). All domains inside a single tree share a common schema (formal definition of all object types that can be stored in an AD deployment) and share a common Global Catalog.
- *Forest* - a grouping or hierarchical arrangement of one or more domain trees that form a disjointed namespace (e.g. cramsession.com and skilldrill.com). All trees in the forest share a common schema and Global Catalog, but have different naming structures. Domains in a forest operate independently of each other, but the forest enables communication across the domains.
- *Sites* - combination of one or more IP subnets connected by high-speed links. Not part of the AD namespace, and contains only computer objects and connection objects used to configure replication between sites.

Site Replication

- Active Directory information is replicated between Domain Controllers (DCs) and ensures that changes to a domain controller are reflected in all DCs within a domain. A DC is a computer running Windows 2000 Server which contains a replica of the domain directory (Member Servers do not).
- DCs store a copy of all AD information for their domain, manage changes to it and copy those changes to other DCs in the same domain. DCs in a domain automatically copy all objects in the domain to each other. When you change information in AD, you are making the change on one of the DCs.
- Administrators can specify how often replication occurs, at what times, and how much data can be sent.
- DCs immediately replicate important changes to AD like a user account being disabled.
- AD uses *multimaster* replication meaning that no one DC is the master domain controller - all DCs within a domain are peers.
- Having more than one DC in a domain provides fault-tolerance. If a DC goes down, another is able to continue authenticating logins and providing required services using its copy of AD.
- Replication automatically generates a *ring topology* for replication in the same domain and site. The ring ensures that if one DC goes down, it still has an available path to replicate its information to other DCs.

Active Directory Concepts

Schema - contains a formal definition of contents and structure of AD such as attributes, classes and class properties. For an object class, the schema defines what attributes an instance of a class must have, additional attributes that are allowed and which object class can be its parent. Installing AD on the first computer in a network

creates the domain and default schema, which contains commonly used objects. Extensions can be made to the schema whenever needed. By default, write access to the schema is limited to members of the Schema Administrators group. (KB# Q229691)

Global Catalog - central repository of information about objects in a tree or forest. AD automatically creates a global catalog from the domains that make up AD through the replication process. Attributes stored in the global catalog are usually those most often used in Search operations (like user names, logon names, etc.) and are used to locate a full replica of the object. Because of this, the global catalog can be used to find objects anywhere in the network without replication of all information between DCs.

Active Directory Naming Conventions

- ***Distinguished Name (DN)*** - every object in AD has one. Uniquely identifies object and contains sufficient info for an AD client to retrieve it from the Directory. Includes the name of the domain that holds the object and also the complete path through the container hierarchy to it. DNs must be unique - AD will not allow duplicates.
- ***Relative Distinguished Name (RDN)*** - if the DN is unknown, you can still query an object by its attributes. The RDN is a part of the name that is an attribute of the object itself (e.g., a user's first name and location).
- ***Globally Unique Identifier (GUID)*** - unique 128-bit number assigned to objects when they are created. The GUID never changes so even if the object is renamed or moved, the GUID can be used to locate it.
- ***User Principal Name (UPN)*** - "friendly name" given to a user account (e.g., johndoe@brainbuzz.com).

Local user accounts: (KB# Q217050)

- Reside only on the computer where the account was created in its local security database. If computer is part of a peer-to-peer workgroup, accounts for that user will have to be created on each additional machine that they wish to log onto locally. Local accounts cannot access Windows XP domain resources and should not be created on computers that are part of a domain.
- Domain user accounts reside in AD on domain controllers and can access all resources on a network that they have been accorded privileges for.
- Built in user accounts are:
  - *Administrator* - used for managing the local system
  - *Guest* - for occasional users - disabled by default
  - *HelpAssistant* – account for providing Remote Assistance
  - *SUPPORT_########* - this is a vendor's support account for the Help and Support Service – disabled by default.

- Usernames cannot be longer than 20 characters and cannot contain the following illegal characters: " / \ [ ] : ; | = , + * ? < >
- User logon names are not case sensitive. You can use alphanumeric combinations to increase security, if desired.
- Passwords can be up to 128 characters in Active Directory (we're not kidding!!) but only 14 characters for a local user account. In either case, Microsoft recommends limiting the length to about eight characters. Read Microsoft's advice on creating strong passwords.
- User accounts are added and configured through the Computer Management snap-in.
- Users should be encouraged to store their data in their My Documents folder that is automatically created within their profile folder and is the default location that Microsoft applications use for storing data.
- Creating and duplicating accounts requires only two pieces of information: username and password. Disabling an account is typically used when someone else will take the user's place or when the user might return.
- Delete an account only when absolutely necessary for space or organization purposes.
- When copying a user account, the new user will stay in the same groups that the old user was a member of. The user will keep all group rights that were granted through groups, but lose all individual rights that were granted specifically for that user.

Local user authentication

Built-in local groups

Local Group	Description
Administrators	Can perform all administrative tasks on the local system. The built-in Administrator account is made a member of this group by default.
Backup Operators	Can use Windows Backup to back up and restore data on the computer.
Guests	Used for gaining temporary access to resources for which the Administrator has assigned permissions. Members can't make permanent changes to their desktop environment. When a computer or member server running Client for MS Networks joins a domain, Windows XP adds Domain Guests to the local Guests group.
HelpServicesGroup	The *SUPPORT_########* (where ######## is replaced by a hexadecimal number) is the only account assigned to this group. It is used by Microsoft Support Services to provide support to your system through the Remote Assistance feature.
Network Configuration Operators	This group is used to delegate the privileges that allow certain users to manage the configuration of networking features.
Power Users	Can create and modify local user accounts on the computer, share resources and can install drivers for legacy software.
Remote Desktop Users	User accounts must be added to this group to be granted the right to log on locally through Remote Desktop Connection.

Replicator	Supports file replication in a domain.
Users	Can perform tasks for which they have been assigned permissions. All new accounts created on a Windows XP machine are added to this group. When a computer or member server running Client for MS Networks joins a domain, Windows XP adds Domain users to the local Users group.

Built-in system groups

Local Group	(SID) Description
Anonymous Logon	(S-1-5-7) A user who has connected to the computer without supplying a user name and password.
Authenticated Users	(S-1-5-11) Includes all users and computers whose identities have been authenticated. Authenticated Users does not include Guest even if the Guest account has a password.
Batch	(S-1-5-3) Includes all users who have logged on through a batch queue facility such as task scheduler jobs.
Creator Owner	(S-1-3-0) A placeholder in an inheritable access control entry (ACE). When the ACE is inherited, the system replaces this SID with the SID for the object's current owner.
Creator Group	(S-1-3-1) A placeholder in an inheritable ACE. When the ACE is inherited, the system replaces this SID with the SID for the primary group of the object's current owner.
Dialup	(S-1-5-1) Includes all users who are logged on to the system through a dial-up connection.
Everyone	(S-1-1-0) On computers running Windows XP Professional, Everyone includes Authenticated Users and Guest. On computers running earlier versions of the operating system, Everyone includes Authenticated Users and Guest plus Anonymous Logon.
Interactive	(S-1-5-4) Includes all users logging on locally or through a Remote Desktop connection.
Local System	(S-1-5-18) A service account that is used by the operating system.
Service	(S-1-5-6) A group that includes all security principals that have logged on as a service. Membership is controlled by the operating system.
Terminal Server Users	(S-1-5-13) Includes all users who have logged on to a Terminal Services server that is in Terminal Services version 4.0 application compatibility mode.

Fast User Switching

This feature is intended for workstations that are configured as standalone units or may participate in a peer-to-peer network (workgroup). Fast User switching allows users to log in extremely quickly without other users having to close their open programs. Once the user has finished doing what he needs to, he can switch back to the previous user whose programs should still be open.
Here are the important points to know for the exam:

- The Fast User Switching Feature cannot be used while participating in a Windows security domain.

- Fast User Switching is not compatible with Offline Files – you can use one or the other, but not both.
- You must be logged on with local Administrative privileges to enable or disable this feature.

Enabling Fast User Switching

Click **Start** > **Control Panel** > **User Accounts**. Next, click the **Change the way users log on or off** button. Select the **Use the Welcome Screen** checkbox – this will make the **Use Fast User Switching** checkbox available – select that as well.

Switching Users

There are three ways to switch users:

1. Click **Start** > **Log Off** > **Switch User**
2. Press **CTRL-ALT-DEL** to open Task Manager and then click **Switch User** on the **Shutdown** button.
3. Hold down the **Windows** key and press the **L** key at the same time. If the computer is not setup for Fast User Switching this key action will lock the computer.

Group Policy

Group Policies are a collection of user environment settings that are enforced by the operating system and cannot be modified by the user. User profiles refer to the environment settings that users can change.
System Policy Editor (poledit.exe) - Windows NT 4, Windows 95 and Windows 98 all use the System Policy Editor (poledit.exe) to specify user and computer configuration that is stored in the registry.

- Not secure because a user can change settings with the Registry Editor (regedit.exe). Settings are imported/exported using .ADM templates.
- Are considered "undesirably persistent" as they are not removed when the policy is no longer applied to systems.
- Do not apply System Policies created using **poledit.exe** to Windows 2000 or XP systems participating in Active Directory. Only use System Policies when Active Directory is not present.

Group Policy snap-in (gpedit.msc) - Exclusive to Windows 2000 and Windows XP, this editing tool is the replacement for the System Policy Editor that was used in the Windows 95/98/ME and Windows NT worlds.

- Group Policies can only be applied to Windows 2000 and Windows XP systems – they are not compatible with previous versions of Windows. If you want to manage policies on legacy Windows clients you will need to use **poledit** instead.
- Settings can be stored locally or in AD. They are secure and cannot be changed by users - only Administrators.

- More flexible than System Policies as they can be filtered using Active Directory.
- Settings are imported/exported using .INF files. The Group Policy snap-in can be focused on a local or remote system.

Incremental Security Templates for Windows XP

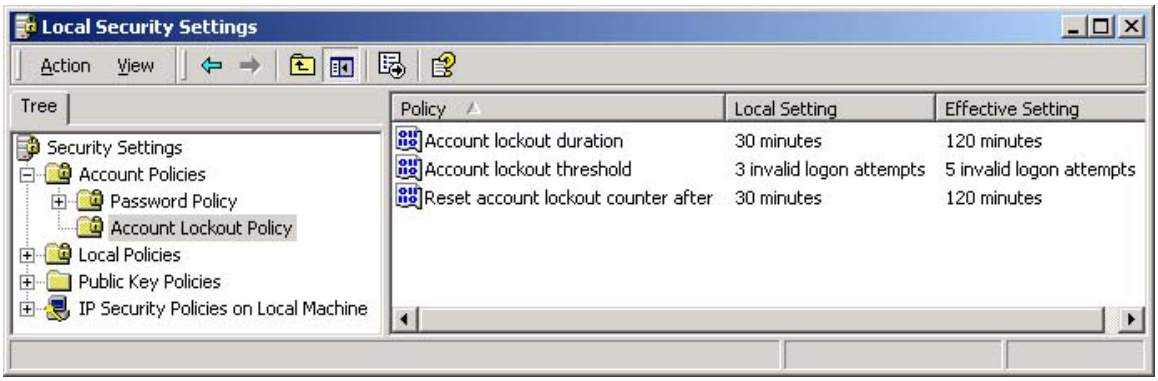
Template:	Filename:	Description:
Default Security	setup security.inf	A computer specific template that represents the default security settings that are applied during installation of the operating system, including the file permissions for the root of the system drive. You can use this template, or portions of it can be used for disaster recovery purposes. Setup security.inf should never be applied using Group Policy.
Compatibility	compatws.inf	Compatibility template, but also referred to in MS documentation as Basic template. Sets up permissions for local users group so that legacy programs are more likely to run. Not considered a secure environment.
Secure	securews.inf	Increases security settings for Account Policy and Auditing. Removes all members from Power Users group. ACLs are not modified.
High Secure	hisecws.inf	Secure template provided for Workstations running in WINXP native mode only. Requires all network communications to be digitally signed and encrypted. Cannot communicate with down level Windows clients. Changes ACLs to give Power Users ability to create shares and change system time.
System Root Security	rootsec.inf	Applying this template restores the default settings to the root of the system drive that XP originally installed with. Use this template to restore default settings. This template will not override setting that have already been defined on child objects. Child objects with no defined settings will inherit the default settings from the root.
No Terminal Server User SID	notssid.inf	The default file system and registry access control lists that are on servers grant permissions to a Terminal Server SID. The Terminal Server SID is used only when Terminal Server is running in application compatibility mode. If Terminal Server is not being used, this template can be applied to remove the unnecessary Terminal Server SIDs from the file system and registry locations. However, removing the access control entry for the Terminal Server SID from these default file system and registry locations does not increase the security of the system. Instead of removing the Terminal Server SID, simply run Terminal Server in Full Security mode. When running in Full Security mode, the Terminal Server SID is not used.

Local Group Policy

- There are two types of Group Policy objects: local Group Policy objects and non-local Group Policy Objects (Active Directory Group Policy). Each Windows XP system can have only one local Group Policy object.
- Order of application is Local, Site, Domain and Organizational Unit. Local Policies have the least precedence whereas OU Policies have the highest (example of Group Policy overriding local policy is shown in Figure 16).

- When a machine is joined to a domain it is assumed that domain settings take precedence over local settings. Local Policy is always overwritten by any existing Group Policies for the same setting that come from the domain.

- Figure 16 – Local Policy Overridden



Config.pol, NTConfig.pol and Registry.pol

- Windows XP uses the **registry.pol** format. Two files are created, one for Computer Configuration (stored in the \Machine subdirectory) and one for User Configuration (stored in the \User subdirectory). Do not edit these files directly – use the Group Policy snap-in to configure the Policy on the local machine.
- **registry.pol** files can be viewed using the **regview.exe** tool from the WINXP Resource Kit. Viewing them does not apply them to the registry.
- **ntconfig.pol** files created with the NT4 System Policy Editor can be applied to Windows XP machines, but this is not recommended. The registry settings in these files are left permanently in the registry. Only do this when Active Directory is not available.
- **config.pol** files are used with Windows 95/98/ME and are incompatible with Windows XP.

Security Configuration

- Security Configuration and Analysis snap-in - Stand-alone MMC snap-in that can configure or analyze WINXP security. Based on contents of a security template created using Security Templates snap-in. There is a text based version of this tool that can be run from the command line - **secedit.exe**.

- By default, Windows XP Professional doesn't require users to press CTRL-ALT-DEL to logon. Increase security by disabling this feature and forcing users to press CTRL-ALT-DEL, which is a key combination recognized only by Windows (set using the Group Policy snap-in).
- To disable access to the workstation, but allow programs to continue running, use the Lock Workstation option (from the CTRL-ALT-DEL dialog box).
- To disable access to the workstation, and not allow programs to continue running, use the Logoff option (from the CTRL-ALT-DEL dialog box).
- To lock the workstation after a period of idle time, use a screensaver password.
- Clicking **Start > Programs > Administrative Tools > Local Security Policy** to enable auditing. In the Local Security Settings window double-click Local Policies and then click Audit Policy. Highlight the event you want to audit and on the Action menu, click Security. Set the properties (success/failure) for each object as desired then restart computer for new policies to take effect.
- Clear the Virtual Memory Pagefile when the system shuts down. By default it is not cleared, but this can be changed under Local Security Policy Settings and will prevent an unauthorized person from extracting information from your system's pagefile. (KB# Q182086)
- Prevent the last user name from being displayed at logon (WINXP Pro does this by default). Use the Group Policy snap-in, Local Computer Policy, to change this.
- When using Event Viewer, only local Administrators can see the security log, but anyone (by default) can view other logs.

Encrypting File System (EFS): (KB# Q223316 & Q230520)

About EFS

- Only available on Windows 2000 and Windows XP operating systems using NTFS partitions and volumes. (NTFS v5).
- Encryption is transparent to the user.
- Uses public-key encryption. Using a public key from the user's certificate encrypts keys that are used to encrypt the file. The list of encrypted file-encryption keys is kept with the encrypted file and is unique to it. When decrypting the file encryption keys, the file owner provides a private key that only he has. (KB# Q241201 & Q230490)
- If the owner has lost his private key, an appointed recovery system agent can open the file using his/her key instead. (KB# Q242296)
- EFS resides in the Windows OS kernel and uses the non-paged memory pool to store file encryption keys - this means no one will be able to extract them from your paging file.

- Encrypted files can be backed up using the Backup Utility, but will retain their encrypted state as access permissions are preserved. (KB# Q227825 & Q223178)
- Microsoft recommends creating an NTFS folder and encrypting it. In the Properties dialog box for the folder click the General tab then the Advanced button and select the "Encrypt Contents To Secure Data" check box. The folder isn't encrypted, but files placed in it will be automatically encrypted. Uncheck the box if you want to decrypt the contents of the folder.
- Although it is recommended that encryption take place at the folder level, it can be done at the file level. Encryption at the folder level will automatically result in all files inside the folder being encrypted. Files moved into or created in an encrypted folder will automatically become encrypted at that time.
- Default encryption strength is 128-bit.
- Compressed files can't be encrypted and vice versa. (KB# Q223093)
- You can share encrypted files under Windows XP Professional by adding the additional users you want to have access to the file after it has been encrypted. (This is not possible under Windows 2000).
- In Windows 2000, Data Recovery Agents (DRAs) were required to implement EFS. In Windows
  XP, they are optional. Microsoft recommends that all stand-alone or domain environments have at least one designated DRA.
- Use the Cipher command to work with encrypted files from the command line. (KB# Q229530)
- The **efsinfo.exe** utility in the WINXP Resource Kit allows an administrator to determine information about encrypted files. (KB# Q243026)

Copying and Moving files encrypted with EFS

Description	Copying	Moving
From one NTFS partition to another NTFS partition on the same computer	Copy the file as normal, it will remain encrypted	Move the file as normal, it will remain encrypted
From an NTFS partition to a FAT partition (includes floppy disks)	Copy the file as normal, it will not be encrypted	Move the file as normal, it will not be encrypted
From one NTFS Windows 2000 computer to another Windows 2000 NTFS computer	Copy the file as normal, it will remain encrypted	Move the file as normal, it will remain encrypted
From one NTFS Windows 2000 computer to another Windows FAT computer	Copy the file as normal, it will not be encrypted	Move the file as normal, it will not be encrypted

Using the CIPHER command

Switch	Function
/a	Performs the specified operation on files as well as folders
/d	Decrypts specified folders and they are marked so files added to them will not be encrypted
/e	Encrypts specified folders and they are marked so any files added later on are encrypted as well
/f	Forces encryption operation on all specified files, even those already encrypted
/h	Shows files with hidden/system attributes (not shown by default)
/i	Continues performing the specified operation even after errors occur. By default, cipher stops when it encounters an error.
/I	Specified operation continues even after errors have been reported
/k	Creates a new file encryption key for users running Cipher command – cannot be used in conjunction with other options
/u	Updates the user's file encryption key or recovery agent's key to the current ones in all of the encrypted files on local drives (that is, if the keys have been changed). This option only works with /n.
/n	Prevents keys from being updated. Use this option to find all of the encrypted files on the local drives. This option only works with /u.
/q	Reports only essential information
/s	Applies the specified operation to sub-folders as well

PathName	Specifies a pattern, file, or folder
/r:PathNameWithoutExtension	Generates a new recovery agent certificate and private key, and then writes them to files with the file name specified in PathNameWithoutExtension. If you use this option, cipher ignores all of the other options.
/w:PathName	Removes data on unused portions of a volume. PathName can indicate any directory on the desired volume. If you use this option, cipher ignores all of the other options.
/?	Displays help at the command prompt.

- **Cipher** cannot encrypt files that are marked as read only.
- **Syntax**: cipher [{/e|/d}] [/s:dir] [/a] [/i] [/f] [/q] [/h] [/k] [/u[/n]] [PathName [...]] | [/r:PathNameWithoutExtension] | [/w:PathName]

IPSec ("Internet Protocol Security"): (KB# Q231585)

- IPSec can be implemented in a Windows 2000/XP domain using Active Directory or on a Windows XP machine through its Local Security settings. This technology was introduced in Windows 2000 and is not available in older versions of Windows.
- IPSec itself is a protocol, not a service. It consists of two separate protocols, Authentication Headers (AH) and Encapsulated Security Payload (ESP). AH provides *authentication*, *integrity* and anti-*replay* but does not encrypt data and is used when a secure connection is needed but the data itself is not sensitive. ESP provides the aforementioned plus *confidentiality* (data encryption) and is used to protect sensitive or proprietary information but is associated with greater system overhead for encrypting and decrypting data.
- Supported IPSec authentication methods are Kerberos v5 Public Key Certificate Authorities, Microsoft Certificate Server, and Pre-shared Key. (KB# Q240262)
- The IPSec Policy Agent is a Windows XP service that runs within the LSASS.EXE process and shows up in the Services snap-in in MMC. It is loaded and started at system startup and retrieves an IPSec policy from either Active Directory or the local registry. After the IPSec Policy has been obtained, it will be applied to *all* IP traffic sent or received by that system (default behavior - IPSec policy can be modified to allow "soft associations" KB# Q234580).
- Before two computers can communicate they must negotiate a Security Association (SA). The SA defines the details of how the computers will use IPSec, with which keys, key lifetimes, and which encryption and authentication protocols will be used.
- When participating in a Windows XP domain, IPSec policies are stored in Active Directory. Without AD, they are stored in these registry keys...

- Group Policy: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent\Policy\Cache
- Local Policy: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent\Policy\Local

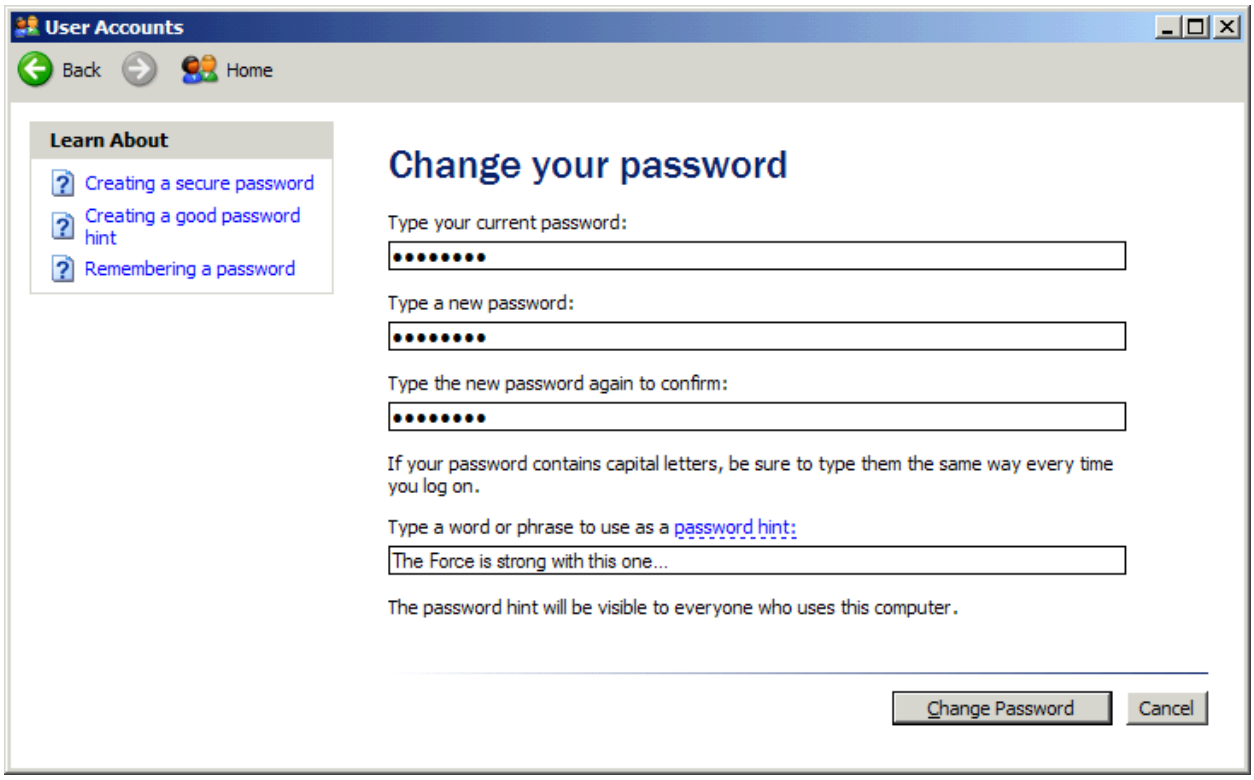
Coping with forgotten passwords

The following features are only available to machines participating in a workgroup. Machines participating in a Windows security domain will not be able to access these features.

Password hints

When changing a password through the **User Accounts** applet in **Control Panel**, you have the option to enter a hint that will help you remember a forgotten password. Keep in mind that this hint is visible to ALL users and drastically lowers your security (shown in Figure 17)
.

Figure 17 – Buddy can you spare a hint?



Creating Password Reset Disks (KB# Q305478)

Windows XP provides users with the ability to create a Password Reset Disk for each user account. To create a Password Reset Disk open the **User Accounts** applet in **Control Panel**. Click the link under **Related Tasks** on the left for **Prevent a forgotten password**. This will start the **Forgotten Password Wizard**. This wizard creates a disk that can be used to reset a forgotten password for a particular account. You do not need to create a new disk each time you change your password; however, when you create a new Password Reset Disk you automatically invalidate all older Password Reset Disks for that account.

Special thanks to Sean McCormick and Will Schmied for contributing this Cramsession. To send feedback to Sean and Will, please post a message labeled "Attention Cramsession Authors" here:
WINXP Professional Forum

Sean and Will would like to acknowledge the following individuals for their assistance in researching this document:

Martin Grasdal
Bruce Ferris
Pat Frank
Editor: Ted Tederoff