Exam
Manual

LearnSmart

Microsoft (70-271) Windows XP User Support

Smarter Training

This LearnSmart exam manual covers all the necessary concepts you must know in order to successfully complete the Support Windows XP OS exam (70-271). By studying this manual, you will become familiar with an array of exam-related content, including:

- Installing a Windows Desktop Operating System
- Managing and Troubleshooting Access to Resources
- Configuring and Troubleshooting Hardware Devices and Drivers
- And more!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual today!

Support Windows XP (70-271) LearnSmart Exam Manual

Product ID: 010277
Production Date: July 12, 2011
Total Questions: 25

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789
solutions@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

This Exam Manual will help you prepare for the Supporting Users and Troubleshooting a Microsoft Windows XP Operating System (70-271) exam. This exam covers topics such as file encryption, offline folders, NTFS, permissions, user accounts, and TCP/IP. These are just a few components found in a Windows XP environment.

What to Know

Exam topics include:

- Perform an attended and unattended installation of Windows XP
- Troubleshoot installation errors
- Upgrade from a previous version of Windows
- Manage and monitor access to resources on NTFS partitions
- Manage share and NTFS permissions
- Configure local and network printing
- Implement offline files
- Configure and troubleshoot devices
- Configure the Windows XP desktop
- Manage and troubleshoot security settings
- Troubleshoot logon errors
- Monitor and analyze system performance
- Configure and troubleshoot TCP/IP
- Implement and troubleshoot ICF
- Troubleshoot name resolution
- Configure and troubleshoot Internet Explorer
- Use Remote Desktop and Remote Assistance

Take time to review the Exam Objectives from Microsoft at:
http://www.microsoft.com/learning/exams/70-271.asp

Tips

This exam consists of 50 questions in a variety of different formats. Questions formats include multiple choice, drag and drop, hot spot, and list and reorder. The exam covers questions configuring, managing, and troubleshooting Windows XP.

In preparing for the exam, you should work with the tools and techniques covered on the exam. In particular, you should set up a workgroup of computers running Windows XP. You should practice with the techniques tested on the exam including installations, Remote Desktop, dial-up remote access, IP addressing, and so on. Some MS books include evaluation editions of Windows XP. You can also use virtual computer software such as Microsoft Virtual PC, in order to set up multiple virtual computers on a single physical machine, and to test different configurations without affecting your production computers. You can download a 45-day free trial of Virtual PC at http://www.microsoft.com/windows/virtualpc/default.mspx

With 90 minutes reserved for the exam, you will have plenty of time to complete the test. You can move back and forth between the questions. This is important to remember because a later question may help you to answer an earlier one that you were unsure about. However, since the exam is timed, you should try to answer each question before moving forward, even if you are unsure of the answer, in the event that you do run out of time. If you are unsure of the correct answer, determine the ones you know are incorrect. This will help you narrow your options and give you a better chance at passing the exam.

Install a Windows Desktop Operating System

Perform and troubleshoot an attended installation of a Windows XP operating system

Answer end-user questions related to performing an attended installation of a Windows XP operating system

There are three different types of Windows XP installations that can be performed:

- Clean installation
- Upgrade from a previous version of Windows
- Multi-boot configuration

A clean installation will overwrite existing data. A clean installation of Windows XP can be invoked by booting directly from the CD-ROM. The advantages to performing a clean install are that it cleans up your computer by getting rid of all the old files and programs that you no longer use and it gets rid of software-related problems you may have been experiencing under the old setup. In other words, your computer is returned to pristine condition as if it had never run an OS before. Generally, performing a clean install results in a more reliable computer. Aside from the amount of time that it takes, one of the downsides to this installation type is that you have to reinstall applications and restore any data that you backed up.

An upgrade can be performed when there is an existing version of Windows installed. The advantage of performing an upgrade is that you can retain all your personal settings and data. With this type of installation, existing user settings configured under the previous version of Windows and applications are retained. Alternatively, if there is an existing copy of Windows installed, you can install Windows XP on a different partition for a multi-boot configuration. This will allow you to return to the previous operating system at any time.

Clean Installation Procedures

To start a clean installation of Windows XP, insert the CD into your CD-ROM drive and restart your computer. When prompted, press any key to boot from the CD. The setup process immediately begins.

The Windows XP setup process occurs in two very distinct phases: the text mode portion and the GUI mode. During the text mode portion of setup, a minimal version of the operating system is loaded into memory. You are prompted to accept the licensing agreement, choose the partition configuration, and select a file system that setup will format the partition with. The setup program copies the system files to the hard drive and places them into the Windows directory. Once complete, your system will restart and the GUI portion of setup will begin.

Once you boot the computer using the Windows XP CD, the text mode phase of setup immediately launches. This step-by-step procedure for the text mode phase typically occurs as follows:

1. Insert the Windows XP CD and restart your computer. Press any key to continue and the setup wizard will launch.
2. The next screen will prompt you to press F6 to install a SCSI or RAID driver. Alternatively, you can press F5 at this point to select the appropriate Hardware Abstraction Layer (HAL) for your computer.
3. Once the initialization process completes, you will be prompted to select the type of installation. Press Enter to continue with the installation of Windows XP.

4. At this point, setup will look for any existing installation of Windows XP. Since this is a clean installation, there should be no existing copies installed.
5. The End-User License Agreement (EULA) will appear. Press F8 to accept the Windows XP Licensing Agreement and continue the setup process. Alternatively, you can press Esc if you do not agree with the EULA. However, you will be unable to continue with the installation.
6. The next screen will display the existing partitions and any unpartitioned space on the computer. To delete an existing partition, use the Up and Down arrows to select the partition, then press D to delete it.
7. Press C to create a new partition. Enter the size of the partition and press Enter.
8. Press Enter to install Windows XP on the selected partition.
9. Next, you must specify the type of file system to use. In most cases, you will want to use NTFS because it is more secure and supports advanced features. Press Enter to continue.
10. After the partition has been formatted and the initialization is complete, you are prompted to press Enter to restart the computer.

At this point, the text-mode phase of setup is complete and the Graphical User Interface (GUI) phase of the setup process will begin.

11. The first screen that will require input from you is the Regional and Language options. Make the appropriate selections and click Next to continue.
12. Type your name and company name. Click Next.
13. Enter the 25-character Product Key. Click Next.
14. Provide a valid computer name and click Next to continue with setup.
15. Select the appropriate day and time settings. This also includes selecting your time zone. Click Next.
16. At this point, the Network Settings screen will appear. Usually you can leave the default option (Typical settings) selected. Click Next.
17. If you are installing XP Professional, the next screen will allow you to configure domain or workgroup membership. By default, the computer will be made a member of a workgroup.
18. The installation of Windows XP will continue.
19. Once complete, your computer will reboot and the Windows Activation screen will appear.

Windows XP can be activated immediately after your computer reboots. Alternatively, you can opt to activate the product at a later time. The activation can be delayed for up to 30 days during which you will receive periodic reminders that the product still needs to be activated. However, after 30 days you are forced to activate Windows in order to gain access to the desktop.

Network-based Installation

To perform a network-based installation, you must set up a distribution server. This is the computer on the network that will host the installation files. There are no real requirements for this computer as long as it is accessible on the network and has sufficient disk space. To set up the distribution server, create a shared folder and copy into it the contents of the I386 folder.

If you are upgrading a previous operating system to Windows Server 2003, you can start the setup process by connecting to the shared folder on the distribution server and running winnt32.exe. If you are performing a new installation, you must boot the system from a network boot disk, which allows the computer to connect to the distribution server or the computer must be configured to boot from a network device.

Once connected to the shared folder on the distribution folder, you can run winnt.exe to start the setup process. As with most commands, there are a number of switches that can be used to modify how the command runs. Some of the common switches that can be used with the winnt.exe command are summarized below.

Switch	Description
/u	Specifies an unattended installation. You must also specify the location of the winnt.sif file.
/s:*Sourepath*	Used to specify the exact location of the installation files.
/t:*Tempdrive*	Specifies where any temporary files should be placed.
/r:*folder*	Specifies an additional folder to be created that remains after setup is complete.
/rx:*folder*	Specifies an optional folder to be copied. This folder is deleted when setup completes.
/a	Enables the accessibility options.

Troubleshoot and complete installations in which an installation does not start

There are a number of different reasons why an installation of Windows XP may not start.

- Bios Issue
  - When the computer restarts, a message will briefly appear on the screen prompting you to press any key to boot from the CD. If this message does not appear and the computer does not boot from the CD, it means you must configure the BIOS to boot from a CD.
  - Some older BIOS will not support bootable CDs natively, but might be upgraded to support it.
  - The BIOS setup settings can be modified using the BIOS setup program. This program is available at system startup by pressing a specific key such as F10.
    - You will need to check your computer manual or motherboard documentation for the exact steps you need to complete to enable your computer to boot from a CD.
- CD-ROM issues
  - Verify that the CD-ROM drive is working correctly.
    - Check to see that the CD-ROM drive is supported by Windows XP.
    - Update the CD-ROM drive firmware.
  - Check Windows XP installation CD.
    - Clean the CD.
    - Obtain a replacement CD.
  - Install Windows XP across the network if you receive CD-ROM errors.

- Network connectivity
  - Verify a network connection is present if installing Windows XP over the network.
  - Locate and browse the Windows XP setup files to verify network connectivity.

Troubleshoot and complete installations in which an installation fails to complete

The setup program needs to copy many files during the installation of Windows XP. It is not uncommon to receive an error during a file copy. This can be caused by a dirty or scratched Windows XP installation CD, a CD-ROM drive that is not working correctly, a virus, and so on.

If you receive a file copy error during setup indicating that a specific file cannot be copied, examine the Windows XP CD to see if there are any scratches. If the CD is dirty or smudged, try cleaning it and then retry the file copy. Conversely, the problem may also be caused by a CD-ROM drive that is not supported by Windows XP. In such cases, replace the drive with a supported one or perform the installation using a different method, such as a network-based install.

Windows XP requires a minimum of 1.5 GB free disk space. If there is insufficient disk space, an error message may appear during setup. You will need to free up disk space by deleting existing files or moving them to another partition. You can also do this during the setup program by formatting the partition, however, formatting the partition will delete all existing files.

Installation problems can also occur if you are attempting to join the computer to a domain. If you are unsuccessful in joining a domain, verify that the computer has a physical network connection. Also make sure that you are typing in the correct domain name and that a computer account exists in Active Directory for the computer. In order to join a domain, a **Domain Name Service** (DNS) server and a domain controller must be available. Check with the domain administrator that these servers are online.

During the installation of Windows XP, several setup log files are automatically created. These files can be used to troubleshoot different problems that may have occurred during setup.

- You can use the following setup log files to troubleshoot an installation of Windows XP.
  - Setupact.log
    - This log file contains all the actions performed during setup in chronological order.
  - Setuperr.log
    - This log file lists any errors that occurred during setup, along with the severity of the error.
  - Comsetup.log
    - This log file provides information about the installation of Optional Component Manager and COM+ components.
  - Setupapi.log
    - This log file provides information about .inf files.

- Netsetup.log
  - This log file lists the actions performed while joining the computer to a workgroup or domain.
- Setup.log
  - The information contained within this log file is used by the Recovery Console.

Perform post-installation configuration

Once you have finished installing Windows XP, the latest service pack should be installed as soon as possible. Microsoft has recently released Service Pack 2 for Windows XP. Many of the updates improve the security of the OS. It includes enhancements to the Windows Firewall, an Internet Explorer Pop-up blocker, and a new Windows Security Center.

Along with having a CD-ROM drive or Internet connection, a computer must meet the minimum requirements for installing Service Pack 2 as listed below:

- 233 megahertz (MHZ) processor
- 64 megabytes (MB) of RAM
- 1.8 gigabytes (GB) free disk space during the installation

Installing a service pack is considered to be a significant process because some of the system files for the operating system are replaced. The installation can result in additional problems because there may be incompatibilities with applications or hardware. For this reason, it is important to plan the installation. Here are a few simple steps you can follow to minimize the problems that can occur from installing updates, hot fixes, patches, and service packs on your systems:

1. Perform a complete backup of your system, and be prepared to perform a full restoration.
2. Read the instructions associated with the update you are installing. It's important to know things such as what the requirements are, applicability to your system, and what the results will be.
3. If possible, perform the installation in a test environment first. Test all applications and hardware to verify compatibility. This will give you a chance to see if there are any negative effects and how to remedy them.
4. If the installation gives you an option to perform a backup in case the installation fails so you can restore certain components to their previous state, be sure to choose Yes.
5. Once the software has been installed, verify that it has done what it was supposed to do. For example, if it is designed to repair a problem, make sure the problem no longer exists.

Perform and troubleshoot an unattended installation of a Windows desktop operating system

Answer end-user questions related to performing an unattended installation of a Windows XP operating system

An unattended installation is performed to automate the installation of Windows XP. There are several different ways that you can perform an unattended installation. You can create an image using Sysprep and deploy it using a third party imaging tool. Conversely, you can use the winnt.exe/winnt32.exe commands and specify an answer file.

An unattended installation can be invoked by typing either of the following commands:

- **winnt32 /Unattend: A:\winnt.sif**
  - This command invokes an unattended upgrade of a previous version of Windows to Windows XP.
- **Winnt /u: A:\Winnt.sif**
  - This command invokes an unattended installation of Windows XP.

System Preparation

One of the benefits of using disk duplication is that it makes installing an operating system, such as Windows XP, on multiple computers more efficient. It is a welcome alternative to manually installing the operating system on multiple computers and configuring identical settings. Instead, the operating system, any service packs, configuration settings, and applications can be included in the image and copied to the target machines.

The System Preparation Tool (Sysprep) included with Windows XP can be used to create the initial disk image. What Sysprep does is prepare the system running Windows XP to be duplicated. Once the image is created, you must then use a third party utility to deploy it.

Using a utility like Sysprep offers several advantages. Although some time must be spent preparing the image, it will obviously speed up future installations as well as reduce the amount of user interaction required. The main disadvantage is that the reference computer and the target computers must have compatible Hardware Abstraction Layers (HALs) and identical Advanced Configuration and Power Interface (ACPI). The size of the hard disk on the destination computer must also be the same size or larger than the reference computer. All plug and play devices are redetected after Sysprep has run.

The general steps that must be completed when using disk duplication to deploy an operating system include:

1. Install the operating system on the reference computer.
2. Configure the reference computer as required.
3. Verify that the reference computer is properly configured.
4. Prepare the computer for duplication using Sysprep and create an optional Sysprep.inf answer file.
5. Duplicate the image.

The first step in using Sysprep to create a disk image is to set up the reference computer. This entails installing the operating system, any service packs, software applications, and configuring settings that you want applied to the target computers. Once you have tested the image and are confident that it's configured the way you want it, you are ready to begin the cloning process.

At this point you are ready to run Sysprep. In order for the utility to function correctly, the Setupcl.exe file, the Sysprep.exe file, and the Sysprep.inf file must all be in the same folder. So your first step will be to create a Sysprep directory in the root folder of drive C on the reference computer. You can create the folder using Windows Explorer or the command prompt. With the second method, open the command prompt and change to the root folder of drive C. Type md Sysprep to create the new directory.

Your next step will be to copy the files required to run the utility from the Windows XP CD to the Sysprep directory you just created. Insert the Windows XP CD into the CD-ROM drive. Open the Deploy.cab file located in the Support\Tools directory and copy the Sysprep.exe file and the Setupcl.exe file into the Sysprep folder.

After completing the steps outlined in the previous section, you are ready to launch the Sysprep utility to clone the reference computer. From the command prompt, change to the Sysprep directory and type in the following command:

Sysprep */optional parameter*

Optional Parameter	Description
-quiet	Sysprep runs without displaying onscreen confirmation messages.
-reboot	Forces the computer to automatically restart after Sysprep is complete.
-audit	Restarts the computer in Factory mode without having to generate new security IDs (SIDs).
-factory	Restarts the computer in a network-enabled state without displaying the Windows Welcome or mini-Setup. Use the parameter to perform configuration and installation tasks.
-nosidgen	The Sysprep.exe file is run without generating new SIDs. Use this parameter if you are not cloning the system.
-reseal	Prepares the destination computer after performing tasks in factory mode.
-forceshutdown	The computer is shutdown after the Sysprep utility is finished.

Once you launch the utility, a warning message will appear. Click OK to acknowledge the warning and the System Preparation Tool window will appear allowing you to configure how the utility will run. The options available here can also be set using command line switches when Sysprep is run from the command prompt.

Once Sysprep has successfully duplicated the reference computer and shutdown (remember the computer can be shutdown automatically by using the -reboot optional parameter), you can remove the hard disk and clone it using third party disk-imaging software.

When you restart a computer from a cloned disk for the first time, two events will occur. First, the Setupcl.exe file will start and generate a new SID for the computer. Second, the Mini-Setup Wizard will start, allowing you to customize the computer. You can also automate this event by creating and using a Sysprep.inf answer file, which can be done using Setup Manager.

Configure a PC to boot to a network device and start installation of a Windows XP operating system

To perform a clean installation of Windows XP across the network, the computer must have a **Network Interface Card** (NIC) that contains a boot ROM that meets the PXE protocol standards. The PXE Network Boot option can be enabled through the computer BIOS.

Alternatively, if the computer does not support booting from the NIC, you can use a PXE emulator boot floppy. The boot floppy can be generated using the **Remote boot disk-generating** utility (rbfg.exe). You can create the disk using the rbfg.exe utility. Insert a blank floppy, type in the path to the rfgb.exe utility (located in the REMINST\Admin\I386 directory on the RIS server), and click create disk. Once the disk is created, you can use it to boot the computer.

In order to perform an installation using this method, a Remote Installation Service (RIS) server must also be present on the network. This is probably the most powerful tool for deploying operating systems because of its flexibility, the operating systems it supports, and its overall ease of use.

The version of RIS that ships with Windows Server 2003 can be used to deploy any of the following operations:

- Windows Server 2003 (all versions)
- Windows XP
- Windows 2000 Server (all versions)
- Windows 2000 Professional

When you use RIS, computers connect to the RIS server during the boot phase and begin the installation of the operating system across the network. The operating system can be installed by using the installation files on the source CD or by using images created with RIPrep.

In order to use RIS to deploy operating systems, the following requirements must first be met:

- There must be an NTFS partition on the RIS server separate from the boot and system partition to store images.
- There must be a DHCP server on the network to assign remote clients and IP addresses.
- A DNS server must be available on the network for clients to locate Active Directory services.
- Active Directory must be installed, as it is required by the RIS servers.

The requirements on the client side are fairly straightforward. They must obviously meet the minimum requirements to install the operating system, have a network card that conforms to the PXE specifications, and the BIOS must be configured to boot from the network card.

The general steps that occur when deploying an operating system using RIS are outlined below. It's a good idea to have an understanding of what occurs, because it will make it easier to troubleshoot problems if and when they do occur.

1. The target workstation is started. During the boot process, using either the PXE-compliant NIC or the RIS boot disk, F12 is pressed to begin the process of remotely installing the operating system.
2. The client receives an IP address and Globally Unique Identifier (GUID).
3. The client is referred to a RIS server on the network.

4. The RIS server queries Active Directory to see if a computer account exists for the workstation. If so, the client is referred to a designated RIS server and prompted for credentials. If no computer account exists, the RIS server that responded prompts the user for credentials.
5. Once the user is logged on to the server, a list of images is displayed and the user can choose the required one.
6. At this point, the installation of the selected operating system begins.

Perform an installation by using unattended installation files

Answer files can help automate the installation of Windows XP. An answer file is a text file that contains answers to various prompts received during the installation of the operating system, thereby eliminating the need for user input.

Creating an answer file is not that difficult because a wizard will walk you through the entire process. The utility used to create the answer file is called Setup Manager. Conversely, if you are skilled in the area of answer files, you can also create one using a text editor such as Notepad.

Before you can use Setup Manager to create the answer file, it must first be installed on your computer. On the Windows XP CD, locate the Support\Tools directory. Open the Deploy.cab file and copy the entire contents to a folder on your computer. Once the files have been copied, you can follow the steps outlined below to create an answer file.

1. Open the folder on your computer that contains the contents of the deploy.cab file and double-click Setupmgr.exe. The Windows Setup Manager Wizard will appear. Click Next.
2. Specify whether to create a new answer file or modify an existing one. If you want to modify one, you must enter the path to the file. Click Next.
3. From the Product to Install dialog box, select Windows Unattended Installation. Alternatively, you can also create a sysprep.inf file. Click Next.
4. Select the platform that you will be using the answer file to deploy. You can select from Windows XP Home Edition, Windows XP Professional, and Windows 2000 Server, Advanced Server, or Data Center. Click Next.
5. Select the level of automation you want to use and click Next.
6. The next dialog box allows you to customize General Settings, Network Settings, and Advanced Settings.
7. Once you have configured all the settings, click Finish.
8. Setup Manager creates the answer file and prompts you to choose a location to save the file. The file can be placed on a floppy disk.
9. Exit the Setup Manager application.

Once the answer file is created, you can open it using a text editor such as Notepad. The file should have the five sections listed below:

- [Unattended]
- [GuiUnattended]
- [UserData]
- [Identification]
- [Networking]

The answer file must be named Winnt.sif and it must be saved to a floppy disk. The floppy has to be inserted into the floppy drive as soon as the computer boots from the CD-ROM.

Upgrade from a previous version of Windows

Answer end-user questions related to upgrading from a previous version of Windows

Windows XP supports a direct upgrade from the following operating systems:

- Microsoft Windows 98
- Microsoft Windows 98 SE
- Microsoft Windows ME
- Microsoft Windows NT Workstation 4.0 with Service Pack 5 can be upgraded to Windows XP Professional, not Home Edition
- Microsoft Windows 2000 Professional can be upgraded to Windows XP Professional, not Home Edition
- Microsoft Windows XP Home Edition

Windows XP does not support direct upgrades for the following platforms:

- Microsoft Windows 3.x
- Microsoft Windows NT Workstation/Server 3.51
- Microsoft Windows 95

Winnt32.exe is used to run Setup on computers running a previous version of Windows that can be upgraded to Windows XP. You can begin the upgrade process by double-clicking winnt32 in Windows Explorer. To perform an unattended upgrade of an operating system to Windows XP, type winnt32 /unattend:*answer_file*.

Verify hardware compatibility for upgrade

Microsoft used to release a **Hardware Compatibility List** (HCL) for its operating systems. The HCL lists all the hardware supported by the operating system. If your hardware is not present on the list, it does not necessarily mean you cannot proceed with the installation, but you should verify with the hardware manufacturer that the component is Windows ready. You can find an up-to-date version of the HCL on Microsoft's website. Microsoft now publishes the **Windows Catalog** that lists the products that have been designed to run on Windows 2000 platforms and later versions.

If you are running a previous version of Windows, an alternative to checking the Windows Catalog is to run the hardware and software compatibility check. You can run the check by inserting the Windows XP CD and choosing the Check system compatibility option or by typing the following command from the command prompt, where x is the letter assigned to your CD-ROM drive:

X:\i386\winnt32 /checkupgradeonly

When you start the actual Windows XP setup, the hardware and software are again checked for any incompatibility issues. Performing the pre-compatibility test is definitely not necessary. However, it's better to know of any issues beforehand than having to halt an installation.

Windows XP Hardware Requirements
Most operating systems are designed to run on a minimum set of hardware requirements to ensure adequate performance. Not meeting these requirements often results in a failed installation. Verify that the hardware in your system at least meets the minimum hardware requirements before upgrading.

The minimum requirements to install Windows XP Professional and Home Editions include:

- 233+ MHZ processor (a maximum of two processors is supported)
- 1.5+ GB free hard disk space
- 64+ MB of RAM (a maximum of 4GB is supported)
- Super VGA or higher resolution monitor
- CD-ROM drive (not required for network-based installations)
- Mouse, keyboard

Keep in mind when you are choosing hardware that these are the bare minimum requirements to run the operating system, and this does not take into account any network services or applications that may be running on the computer. Plan to increase these requirements for optimal performance.

Verify application compatibility for upgrade

Before you upgrade to Windows XP, you should verify that any applications currently running will still function after the upgrade is complete. Most new programs will not be affected by the upgrade. However, older programs may not function correctly under Windows XP.

If you have the Windows XP CD, you can run the Windows XP Upgrade Advisor before performing the upgrade. From the Welcome to Microsoft Windows XP dialog box shown in the figure, select Check system compatibility.

Figure: Check system compatibility

If you have problems running programs after Windows XP is installed, you can use the Program Compatibility Wizard. You can run the Program Compatibility Wizard before you try other ways of updating your programs or drivers because it identifies compatibility fixes written specifically for Windows XP.

If a compatibility problem prevents you from installing a program on Windows XP, run the Program Compatibility Wizard on the Setup file for the program. The file may be called Setup.exe or something similar, and is probably located on the Installation disc for the program.

To run the Program Compatibility Wizard, follow these steps:

1. Click Start, point to All Programs, point to Accessories, and then click Program Compatibility Wizard.
2. Follow the wizard's instructions to select the program's executable file, choose a compatibility mode, set the visual options, and then test the program.

The wizard prompts you to test your program in different modes and with various settings. For example, if the program was originally designed to run on Windows 95, set the compatibility mode to Windows 95 and try running your program again. The wizard also allows you to try different settings, such as switching the display to 256 colors and the screen resolution to 640 x 480 pixels. The wizard will launch your program with the selected settings, and allow you to test how the program works. The final page of the wizard enables you to select whether to permanently apply the compatibility settings, abandon the changes, or save them and run the wizard again to apply different settings. It is likely that you will need to repeat this process until you find the correct compatibility mode.

As an alternative to running the Program Compatibility Wizard, you can set the compatibility properties for a program manually by following these steps:

1. Right-click the program icon on your desktop or the shortcut on the Start menu for the program you want to run, and then click Properties.
2. Click the Compatibility tab, and change the compatibility settings for your program.

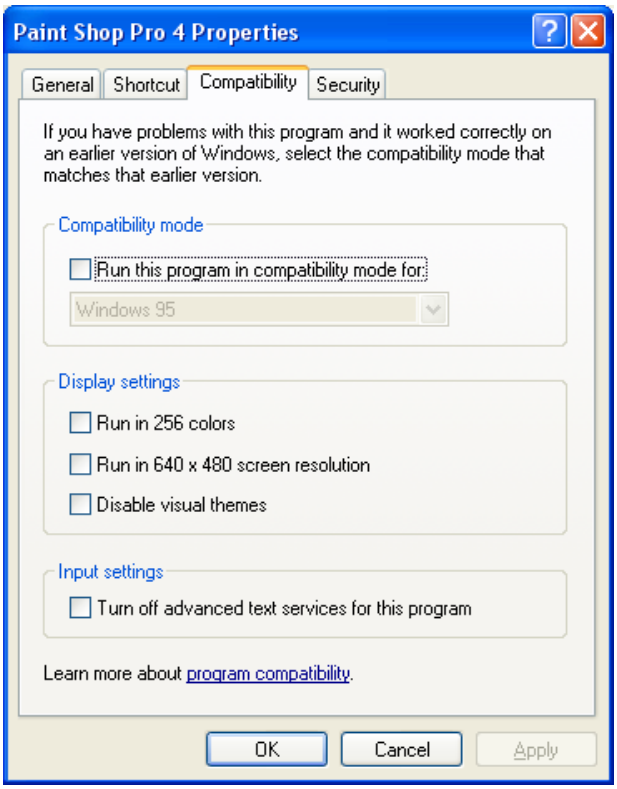

Figure: Compatibility tab used to configure application compatibility settings

The Compatibility tab is only available for programs installed on your hard drive. Although you can run the Program Compatibility Wizard on programs or Setup files on a CD-ROM or floppy disk, your changes will not remain in effect after you close the program. For more information about an option on the Compatibility tab, right-click the option and then click What's This.

QFIXAPP, also known as Microsoft's **Quick Fix Utility**, is an application included with the Application Compatibility Toolkit for Windows XP and Windows Server 2003. Essentially, what the utility does is allow you to browse through various appfixes and apply the fixes on an as-needed basis. The nice thing about using this utility as opposed to the Program Compatibility wizard is that QFIXAPP is non-wizard based. Non-Wizard based utilities tend to provide you with more control. It's also a really good tool for tweaking those applications that don't appear on the list of applications with known issues operating under Windows XP.

For more information about the utility, visit the following URL: http://support.microsoft.com/kb/317510.

Another useful application included with the Application Compatibility Toolkit is called CompatAdmin, or the **Compatibility Administrator Program**. Like the QFIXAPP, you can use the tool to browse through various application fixes and apply them as needed. It also allows you to distribute the fixes to a large number of computers. You can find more information about CompatAdmin at the following URL: http://www.microsoft.com/technet/prodtechnol/winxppro/plan/appcmpxp.mspx.

Migrate user state data from an existing PC to a new PC

Windows XP makes it very simple to move from an old computer to a new one. Many people are often reluctant to get a new computer because they do not want to lose their existing files and settings. You can use the Files and Settings Transfer Wizard included with Windows XP to move settings from one computer to another.

The Files and Settings Transfer Wizard eliminates the need for you to completely reconfigure all of the user's personalized settings on a new computer. It can be used to transfer personalized settings such as display, dial-up connection, Outlook Express, and Internet Explorer settings. It can also be used to move folders such as My Documents and other files to the new computer.

The old computer and the new must be connected in some way to run the wizard. If both computers have **network interface cards** (NICs), connect them using a hub or cross-over cable. Otherwise, you can use a direct cable connection.

The first step is to save the files and settings on your existing computer using the Files and Settings Transfer Wizard.

1. Insert the Windows XP CD. If AutoRun is enabled, click Perform Additional Tasks.
2. Open Windows Explorer and open the Support/Tools directory on the Windows XP CD.
3. Double-click Fastwiz.exe. This launches the Files and Settings Transfer Wizard.
4. Click Next.
5. Select Old computer and click Next.
6. Select the method you want to use to transfer your files and settings. Click Next.
7. Select the items you want to transfer. Click Next.
8. If necessary, insert the required media and click Ok.
9. Click Finish.

The next step will be to transfer your selected files and settings to the new computer.

The first step in getting your new computer ready is to choose the files and settings you want to transfer.

Once you have done this, you are ready to transfer them to your new computer using the steps outlined below:

1. Log on to your new Windows XP computer.
2. Click Start. Point to All Programs, Accessories, System Tools, and select Files and Settings Transfer Wizard. Click Next.
3. Select New computer. Click Next.
4. Click I don't need the Wizard Disk. I have already collected my files and settings from my old computer. Click Next.
5. Select the transfer method you used to collect your files and settings. Click Next.
6. Click Finish.
7. Click Yes to log off the computer.

Once you log back on to the computer, your files and settings from your old computer are transferred to the new one. Keep in mind though that it does not transfer your applications. Applications should be installed on the new computer before migrating settings.

The Files and Settings Transfer Wizard is suitable for small-scale migrations. However, in cases where there are a large number of computers that need to be migrated, you can use a utility called the **User State Migration Tool** (USMT). A major difference between the two utilities is that USMT is not able to copy settings directly from one computer to another. It does require an intermediary store. USMT can also automate the process of capturing user state data.

Install a second instance of an operating system on a computer

Multiple operating systems can be installed on a single computer. This is referred to as **multi-booting.** Each time a user boots the computer, they can choose which operating system to start.

- Windows XP must be installed on a separate partition. Otherwise, files used by the other operating system will be overwritten.
- Applications must be installed under each operating system.
- If multi-booting Windows XP and MS-DOS, MS-DOS should be installed first and the system partition must be formatted with FAT.
- If multi-booting Windows XP and Windows 95, install Windows 95 first and then format the system partition with FAT.
- If multi-booting Windows XP and Windows 98, install Windows 98 first. The system partition can be FAT or FAT32.
- If multi-booting more than one instance of Windows XP, or Windows XP and Windows 2000, install each instance on a separate partition.

Managing and Troubleshooting Access to Resources

Monitor, manage, and troubleshoot access to files and folders

Answer end-user questions related to managing and troubleshooting access to files and folders

Windows XP supports three different file systems: NTFS, FAT32, and FAT. For most situations, it is definitely recommended that you opt to use NTFS because it includes some important features not included with the other two.

Some of the features included with NTFS that make it a more powerful file system include:

- File and folder security. Permissions can be set on individual files as well as folders unlike FAT and FAT32, which on support permissions at the folder level.
- Disk compression. Disk compression allows you to compress folders, files, and even entire drives to save space.
- File Encryption. The contents of folders and files can be encrypted to increase security. Only the individual who encrypted the contents is able to view them.
- Disk Quotas. Allows you to monitor and control the amount of disk space being consumed by users.

In most cases, the only time you would want to use FAT or FAT32 is for multi-boot configurations where you have Windows XP and an older operating system, such as Windows 98, running on the same system. There is a one-time conversion from FAT or FAT 32 to NTFS, leaving all the files on the partition intact. You can convert a partition to NTFS using the Convert command. The syntax is convert *x*: /fs:NTFS where x is the drive letter assigned to the partition you want to convert.

Monitor, manage, and troubleshoot NTFS file permissions

NTFS permissions include standard permissions and special permissions. The standard permissions are actually a combination of specific special permissions.

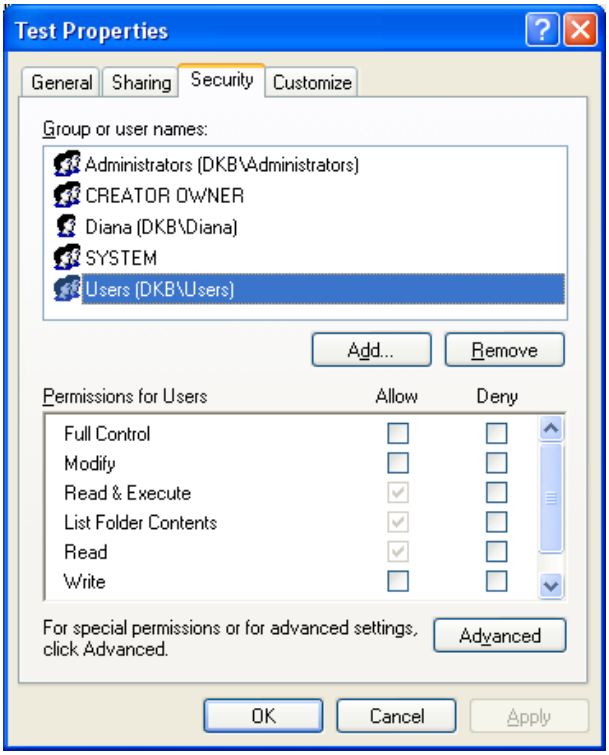

Figure: Standard NTFS permissions

The Standard NTFS permissions are as follows:

- **Read -** Allows a user to view the contents of a folder and the contents of a file. The user cannot view the contents of subfolders.
- **Write -** Allows a user to create files and folders, but not read the contents of any files and folders they did not create.
- **Modify** - A full combination of both Read and Write permissions. A user can also delete files within a folder that has this permission. They can also view the contents of subfolders.
- **Read & Execute -** The Read permission allows the ability to read file and folder permissions, along with the contents of subfolders.

- **List Folder Contents -** The same as Read & Execute, without the ability to execute files.
- **Full Control -** Allows a user to read, execute, create, and delete data, along with the added ability to assign other user accounts permissions to the object.

Each of the standard permissions is actually composed of several Special Permissions. These permissions can be viewed or modified by clicking on the Advanced button.

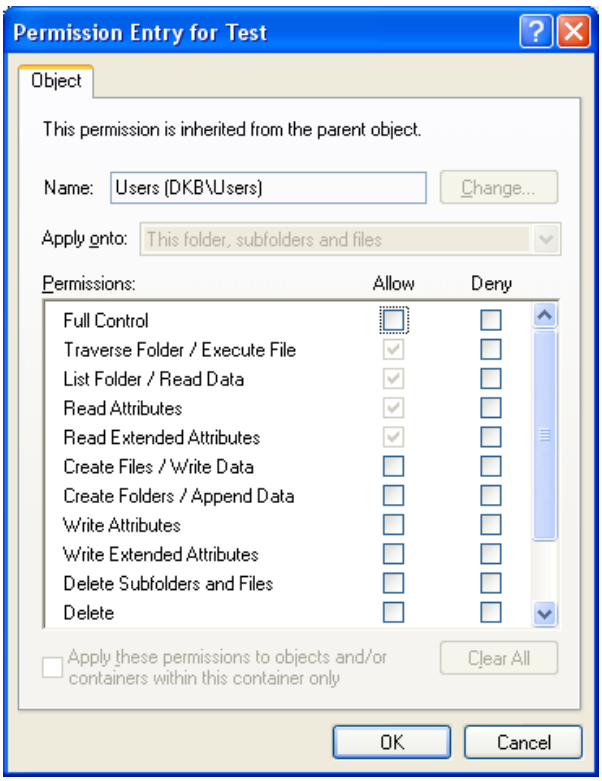

Figure: NTFS Special Permissions

Windows XP has added the additional Special Permissions to the permissions list in order to indicate any advanced permissions that have been assigned to the selected user or group. Special permissions can be used in combination with any standard permission to provide a more granular approach to file and folder security. With some research, you can determine which special permissions make up the standard permissions, as shown in the table below. While you do not need to spend time memorizing the information in the table, it is useful in understanding the relationship between standard and special permissions.

	Read	Write	List Folder Contents	Read & Execute	Modify	Full Control
Traverse Folder/ Execute file			x	x	x	x
List Folder/ Read Data	x		x	x	x	x
Read Attributes	x		x	x	x	x
Read Extended Attributes	x		x	x	x	x
Create Files/ Write Data		x			x	x
Create Folders/ Append Data		x			x	x
Write Attributes		x			x	x
Write Extended Attributes		x			x	x
Delete Subfolders & Files						x
Delete					x	x
Read Permissions	X		x	x	x	x
Change Permissions						x
Take Ownership						x

A folder or file on an NTFS partition can be shared from the folder or file's properties dialog box. Click the Security tab to configure the permissions you want to assign to various users and groups.

Moving/Copying Folders

NTFS permissions can be affected when you copy or move a folder or file within or between NTFS partitions. What you really need to remember though is this — the only time a folder or file will retain its original permissions is when it is moved within the same NTFS partition. Let's take a look at an example:

Two folders, Private and Public, are stored on F (and F is an NTFS partition). There is a file called Employees.doc stored in the Private folders. Users have been assigned Read permission. However, users have been assigned Full Control to the Public Folder. When Employees.doc is moved from the Private folder to Public, it will retain its original permission (in this case, Read).

All other actions will result in a permission change. If you copy a folder or file within the same NTFS partition, the folder or file will inherit the permissions of the destination, and the original permissions are lost. If you copy or move a folder or file between NTFS partitions, the original permissions are also lost, and the permissions of the destination folder are inherited. If you move a folder or file to a FAT partition, obviously the NTFS partitions will once again be lost.

Permission Inheritance

Windows XP uses permission inheritance to simplify administration. By default, permissions applied to a parent folder are passed on to any subfolders and files within it.

You can change the default behavior and prevent permissions from being passed on to a subfolder. You can accomplish this by opening the properties dialog box for a folder, selecting the Security tab, and clicking the Advanced button. From the Permissions tab, deselect the option to Inherit from parent the permission entries that apply to child objects.

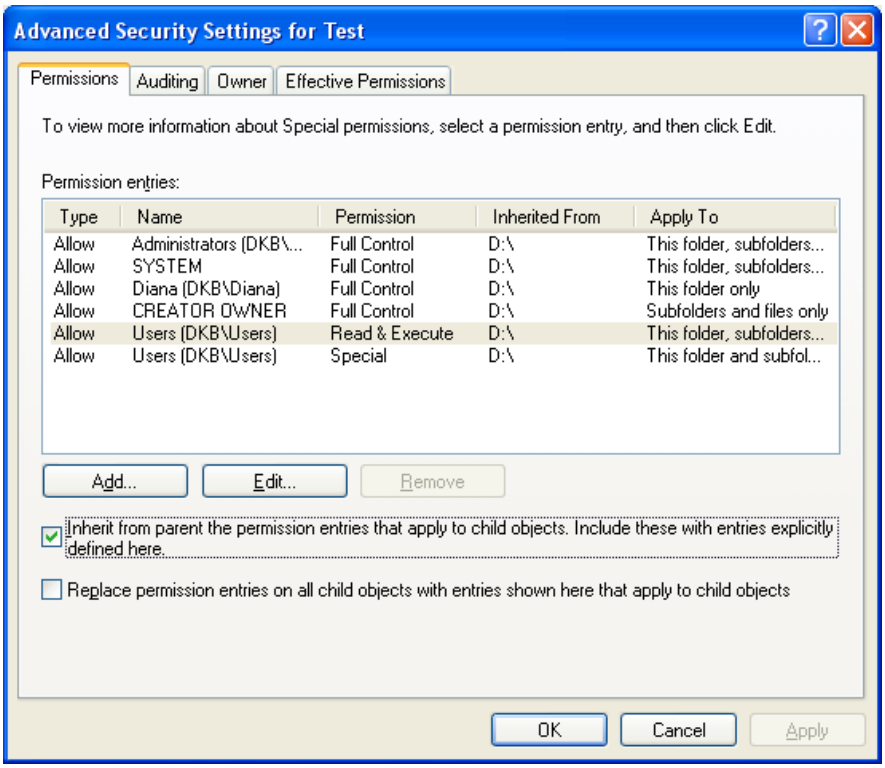

Figure: Permission Inheritance

Manage and troubleshoot simple file sharing

When simple file sharing is enabled, you can share folders with all users in your workgroup and make folders in your profile private. Once you share a folder, all users on the network are allowed access to it. However, if you want to prevent specific users and groups from accessing your folders and files, simple file sharing must be disabled. Once simple file sharing is disabled, the Security tab will be available from the properties dialog box for a folder or file. You can use this tab to set permissions for users and groups. The Security tab is only available if simple file sharing is disabled. You can disable simple file sharing with Windows Explorer by selecting Folder Options from the Tools menu. From the View tab, clear the check beside Use simple file sharing (recommended).

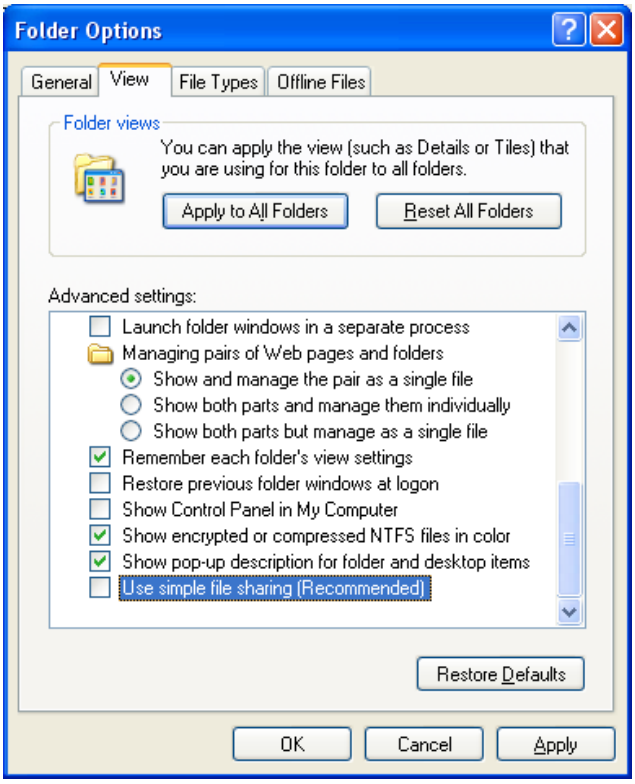

Figure: Disabling Simple File Sharing

Manage and troubleshoot file encryption

One of the ways in which you can protect your files is to use file encryption. Once you encrypt a file, it is only readable by you, even if an attacker bypasses the operating system by removing the hard disk or booting to a different operating system. Anyone else who attempts to open the file will be unsuccessful. Windows XP Professional supports file encryption by using a technology called Encrypting File System (EFS). This feature is not included with Windows XP Home edition and can only secure folders and files on an NTFS partition. Once a folder is encrypted, only the user who encrypted it can view the contents. All other users, unless explicitly given permission to transparently access the file, will receive an access denied message. If you encrypt a file, it is automatically decrypted for you when you open it. In other words, the process of decrypting the file is completely transparent to you.

To encrypt a file using Windows XP Professional:

1. Open My Computer.
2. Right-click the file you want to encrypt and click Properties.
3. Click the Advanced button on the General tab.
4. Select the option to Encrypt contents to secure data. Click Ok.
5. Click Ok to close the file's properties window.
6. From the Encryption Warning window, choose whether to Encrypt The File Only or to Encrypt The File And The Parent Folder. If the folder is encrypted, any new files saved into the folder will automatically be encrypted.
7. Click OK.

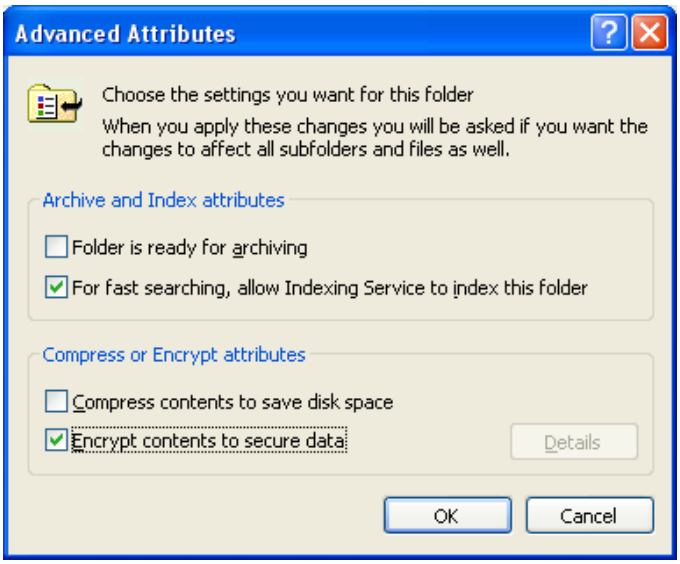

Figure: Encrypting a folder on an NTFS partition

Other users can be given access to an encrypted file using the steps described below:

1. Right-click the encrypted file that you want to share and click Properties.
2. From the General tab, click the Advanced button.
3. From the Advanced Attributes dialog box, click the Details button.
4. Click the Add button.
5. Select the user to whom you want to grant access to the encrypted file.
6. Click OK three times.

Once the appropriate user has been granted permission, they will be able to view the contents of the encrypted file while all other users are still denied access.

Use the following points when troubleshooting file encryption:

- The user who encrypted a folder or file can open it. All other users are denied access unless they have explicitly been granted access.
- Encryption is only available on NTFS partitions.
- System files cannot be encrypted.
- A user with the Delete permission can delete an encrypted file, even if they don't have access to decrypt the file.
- Recovery agents can decrypt files if a user loses their private key.
- Files can be encrypted from the command line using the Cipher command.
- Encrypt a folder and all files added to the folder will be encrypted.
- An encrypted file cannot be shared or compressed.

Manage and troubleshoot access to shared folders

Answer end-user questions related to managing and troubleshooting access to shared folders

In order for a folder to be accessible to other users on the network, it must be shared. Once a folder has been shared, you can configure the share permissions to control the type of access users and groups will have. Share permissions include:

- Full Control
  - Allows a user to create, delete, modify, and grant share permissions.
- Read
  - Allows a user to read the contents of a folder, but not modify any contents. Users cannot create files either.
  - By default, the Users group is assigned Read permission to a shared folder.
- Change
  - Allows a user to create, delete, and modify the contents of a folder. This includes creating documents and subfolders.

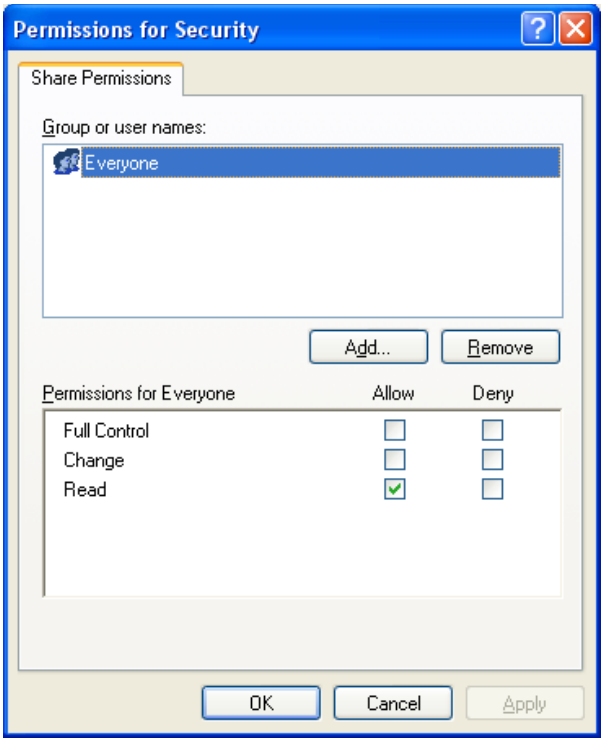

Figure: Share permissions

Create shared folders

A shared folder can be created within Windows Explorer using the steps outlined below. By default, the Everyone group is granted Read permission to a shared folder.

1. Right-click the appropriate folder and click Properties.
2. Select the Sharing tab.
3. Click the Share This Folder option.

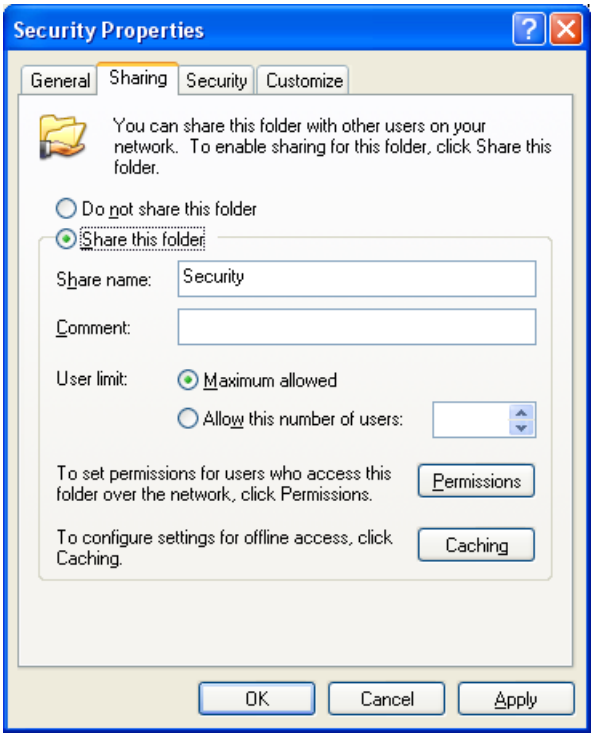

Figure: Creating a shared folder

4. Click the Permissions button to specify which users and groups have access to the folder and the type of access they will have.
5. Click OK.
6. To limit the number of users who can simultaneously connect to the share, click Allow This Number Of Users, and then type the number of users who can connect to the shared folder at one time.
7. Click OK.

Another method of sharing a folder is to use the Shared Files Wizard. This method is useful if you are sharing several folders.

You can launch the Shared Files wizard using the following steps:

1. Click Start and select Run.
2. Type shrpubw.exe and click OK.
3. The Create A Shared Folder Wizard appears. Click Next.
4. On the Set Up A Shared Folder page, click Browse to specify the location of the folder you want to share. Then, click OK.
5. Type in a share name and a description.
6. Click Next.
7. Specify the type of permissions, and then click Next.
8. Click Finish.

You can also share and stop sharing resources from the command prompt. This is accomplished using the 'net share' command. To share a resource using this method, open the command prompt from the Accessories submenu on the Start menu. Next, type in the 'net share *sharename=folder*'. For example, to share a folder on your D drive called Files, simply type the following at the command prompt:

net share Files=d:

Hidden Shares

Shared folders are visible to users on the network through My Network Places. A folder can be shared but remain hidden to users on the network by appending a dollar sign character ($) to the end of the share name.

The shared folder is only accessible to users on the network if they know it exists. It will not be visible within My Network Places. In order to access the folder, users must type in the path and the share name. For example, \\MyComputer\SharedFolder$. If you omit the dollar sign character at the end of the share name when typing in the path to the folder, the resource will not be found.

Changing the Share Name

If you wanted to change the share name of a folder, you would probably open the properties dialog box for the folder and try to type in a new name. However, a share name cannot be changed using this method.

Once you share a folder by selecting the Share this folder option, type in the share name, and click OK; the share name is set. In other words, it cannot be changed this way. In order to change the share name assigned to a shared folder, you must stop sharing the folder first by selecting the Do Not Share This Folder option, and then click OK.

Now you have to complete the steps you followed when you initially shared the folder. This means opening the properties dialog box for the folder and selecting the Share This Folder option. At this point, you can type in the share name you want assigned to the folder. Unfortunately, you will also have to reset any specific share permissions you had configured. Additionally, users will have to re-connect to the shared folder.

Configure access permissions for shared folders on NTFS partitions

Multiple NTFS permissions are cumulative. They stack upon each other, and the highest permission is the effective permission. Share permissions work the same way. However, when you combine NTFS permissions and share permissions, the most restrictive permission between the two becomes the effective permission.

For example, Jane has been denied all access share permission to a specific folder. She has full control NTFS permission to the same folder. The result is that she has no access to the folder because the share permission is the most restrictive permission. Now, reverse the situation. Jane has Full control share permission to the same folder, but Deny all NTFS permission. Jane will first encounter the share permission, which permits access and lets her through to the NTFS permissions, but she will stop at that point because the NTFS permissions won't allow any access. These are pretty clear-cut examples.

Here is a more difficult example: Jane has Read share permission to the folder, but Change NTFS permission. When Jane encounters the share permission, she is granted Read and moves on. Because the share permission is Read only and more restrictive than the NTFS permission, the NTFS permission cannot override it. Therefore, she accesses the data with Read only permissions. If NTFS and share permissions are reversed in this example, Jane will still only have Read permission.

You also need to consider group memberships. This is one place where the Effective Permissions tool included with Windows XP becomes very useful. The Effective Permissions essentially runs through each membership-inherited share permission, takes the most permissive share permission, runs through each membership-inherited NTFS permission, takes the most permissive NTFS permission, and then runs the two of them through the share-first, NTFS-last procedure above.

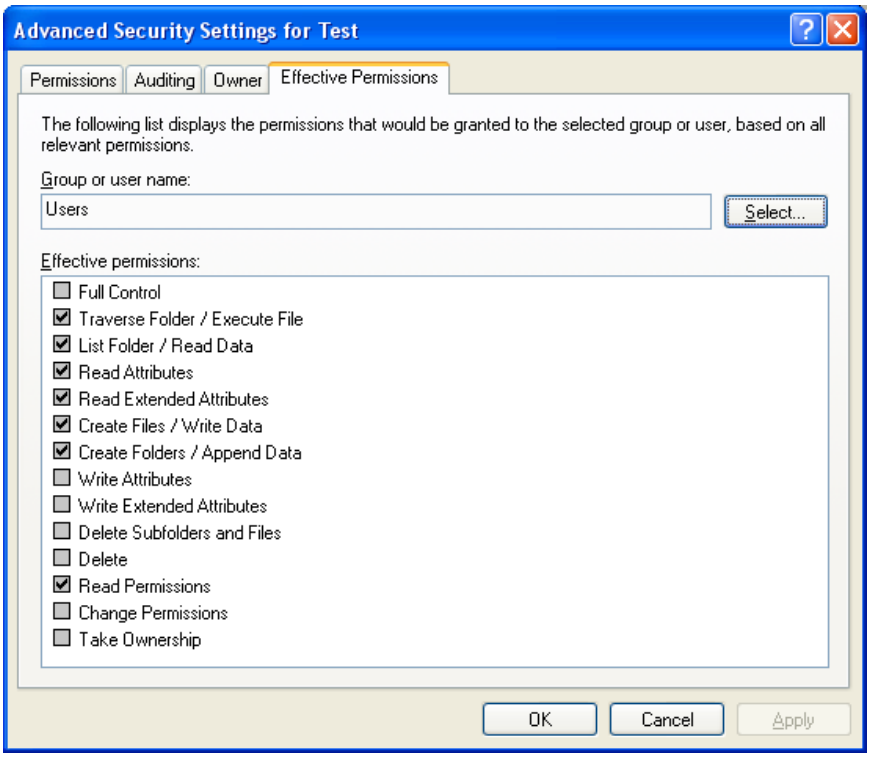

Figure: Identifying Effective Permissions

Troubleshoot and interpret Access Denied messages

Access denied messages can appear for several different reasons, such as a user attempting to access a folder or file without sufficient permissions, or a user attempting to access a file that has been encrypted by another user. Access denied messages that appear when accessing a resource are the result of a permission conflict. In such situations, it is useful to use the Effective Permissions tool to determine the permissions assigned to the user. You should also check the groups that the user is a member of because permissions assigned to groups are inherited by the group's members.

Auditing is a security feature that allows you to track events that occur on a computer. For example, you can monitor all successful and unsuccessful log on attempts. If you have shared resources on a computer, you can use auditing to monitor access to them. In order to do this, you must first enable auditing and then enable auditing of your specific shared resources.

In Windows XP, auditing can be enabled using the steps below:

1. Within the Control Panel, open the Administrative Tools applet.
2. Double-click Local Security Policy.
3. Under Local Policies, click Audit Policy.
4. Double-click Audit object access.
5. Click Success and/or Failure.
6. Click OK. Close the Local Security Policy console.

Now that auditing is enabled, you must then enable auditing on your specific resources.

7. Open Windows Explorer.
8. Browse to the appropriate folder.
9. Right-click the folder and click Properties. Select the Security tab.
10. Click the Advanced button and select the Auditing tab.
11. Click the Add button to specify which users and groups you want to audit.
12. Type in the user or group name and click Check Names. Click OK.
13. Specify the type of events you want to audit by placing a check beside each one. Click Ok.
14. Click OK to close the Advanced Security Settings dialog box.
15. Click OK to close the folder's properties dialog box.

Once auditing is set up on a computer, any security related events that occur will be written to the security log. You can view the contents of the log file using the Windows Event Viewer. You can open the Event Viewer applet by opening the Control Panel, double-clicking Administrative Tools, and double-clicking Event Viewer. Click Security, and all the audited events that have occurred will be displayed in the details pane.

Connect to local and network print devices

Answer end-user questions related to printing locally

Before you actually get into printer installations and management, you should become familiar with some of the common print terms that you are likely to encounter.

- Logical Printer
  - When you encounter this term, understand that Microsoft is referring to the software that sends the print jobs from the client computer to the print server. The term is often used interchangeably with 'printer'. Logical printers appear within the Printers and Faxes folder. If you right-click on a logical printer and select properties, you can configure various options for the physical print device.
- Print Device
  - The term 'print device' is referring to the physical printer that is attached to a computer. You may encounter other documentation that refers to the print device as the physical printer.

- Print Server
  - The print server is the computer that is hosting the print device. In other words, the physical printer is attached to it. The print server receives print jobs from clients on the network, stores them in the spool until the printer is available, and sends the print jobs from the spool to the print device. A print server is any computer hosting a print device that has been shared, making it accessible to other clients on the network.
- Network-attached Printer
  - A network-attached printer is a physical printer that is connected directly to the network. It has its own network interface, so it can be connected to the network using a network cable, as opposed to being connected through another computer.
- Spooler
  - The spool, or print spool, is where print jobs are stored until they can be sent to the print device. Most operating systems, including Windows, have its own spool. The spooler is the software that manages the spool. The spooler saves print jobs to a file and sends print jobs from the spool to the print device.

The process that occurs when a document is sent to a print device is complex. The printing process is divided into three phases:

- Client processes
- Spooler processes
- Printer processes

The following steps outline the general process that occurs when a Windows XP-based client submits a print job.

1. A user submits a print job from an application.
2. The application used to initiate the print job interacts with the print driver and graphical device interface (GDI) to create a print job. The print job must be suitable for the logical printer selected by the client.
3. The print job is delivered to the spooler.
4. The client side spooler (Winspool.drv) makes a call to the server side spooler (Spoolsv.exe) on the local computer.
5. The server side spooler calls the print router (Spoolss.dll).
6. The print router is responsible for directing print jobs to either the local print provider (LPP) or the remote printer server. The router passes print jobs for a local printer to the local print provider. It passes print jobs for a remote printer to the print server.
7. The local print provider writes the print job to a spool file (SPL).
8. The print processor despools the print job. It performs any additional modifications to make the document print properly.
9. The print job is sent to the page separator. A separator page is added if it is required.
10. The print job is sent to the appropriate port print monitor. It manages the connection port and the language used by bi-directional print devices.
11. The print device receives the print job and prints the data.

Configure and manage local printing

Windows XP supports plug and play technology. This means that if your printer is connected using USB or IEEE 1394 compatible port, it is automatically detected. Windows XP will automatically install the printer drivers and configure the printer for you. The logical printer will appear within the Printers and Faxes folder where you can make any changes to its configurable properties.

When installing a local print device, you should have a few key pieces of information readily available including:

- The make and model of the print device you are adding
- The port which the print device is connected
- Updated print drivers
- The name you will assign to the logical printer

Once you have the necessary information, you are ready to add the printer. Before you launch the Add Printer Wizard, physically attach the print device to your computer and turn it on. Then you can complete the steps listed below.

1. Click Start and click Printers and Faxes.
2. Under the list of Printer Tasks, click Add a printer. This launches the Add Printer Wizard.
3. Click Next.
4. Verify that Local printer attached to this computer is selected. Click Next.
5. Use the drop down arrow to select the port. Click Next.
6. Select the Manufacturer of your printer and the model. Click Next. If your printer is not listed, click the Have Disk button. You'll need to locate the manufacturer-supplied drivers on your computer or disk.
7. Type in a name for the printer. This is the name that will appear under the printer icon in the Printers and Faxes folder. Click Next.
8. If you want to share the printer, click Share name. Type in the share name for the printer. Click Next.
9. If you share the printer, type in the location and comment. Click Next.
10. Click Yes if you want to print a test page. Click Next.
11. Click Finish at the Summary window.

Print Management

Print management can be broken down into two different categories: server management and document management. Server management entails configuring the print server properties. Document management on the other hand, involves managing the documents that are currently in the print queue.

Windows XP can function as a print server. To access the print server properties, open the Printers and Faxes folder and click Server Properties from the File menu. The Print Server Properties dialog box has four different tabs: Forms, Ports, Drivers, and Advanced.

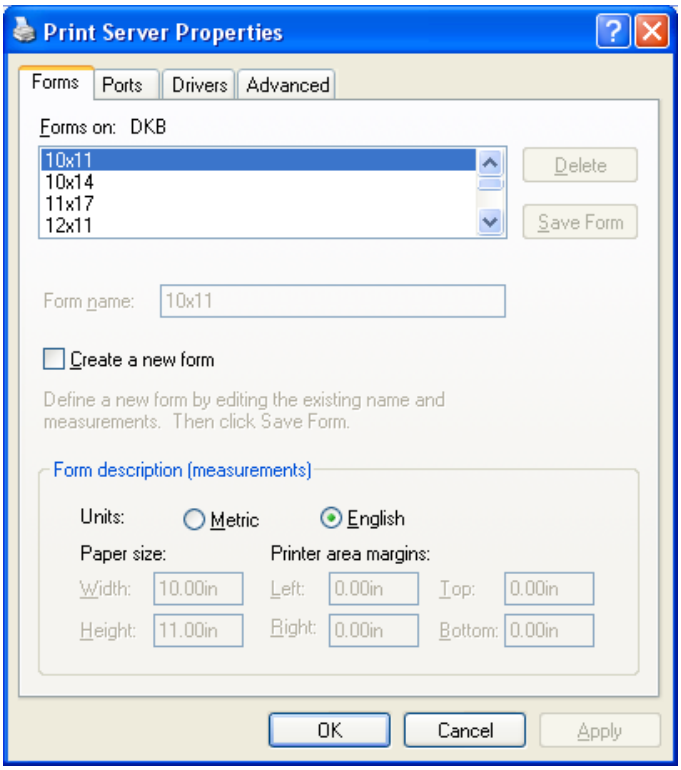

Figure: Print Server Properties Dialog Box

Using the Forms tab, you can configure the options below. A form is a paper type with a specific size and margins.

- Delete existing print forms on the print server.
- Create a new form. If you create a new form, you have to specify a name, paper size, and margins.

From the Ports tab, you can configure the following settings:

- Add new ports.
- Delete existing ports.
- Configure the existing ports. The port settings will vary depending on the type of port you are configuring.

The Drivers tab lists all the printer drivers that are currently installed on the print server. From here, you can install printer drivers for different platforms, remove or replace existing drivers, and configure printer driver properties.

Finally, from the Advanced tab you can do the following:

- Change the location of the spool file. The default location is %systemroot%\System32\spool\Printers.
- Log spooler events. All events are written to the System log.
- Log spooler warning events.
- Log spooler information events.
- Beep on errors of remote documents.
- Show informational notifications for local printers.
- Show informational notifications for network printers.
- Printer notification. When a document has printed, notification can be sent to the user or the computer.

You can manage the print jobs on the print server through the Print Queue window. You can access a print queue for a logical printer by double-clicking the appropriate printer icon in the Printers and Faxes folder. The following commands are available from the Documents menu:

- Pause - The document remains in the queue but it is not printed.
- Resume - This command will "unpause" a document.
- Restart - The print process starts over. The current print process is stopped.
- Cancel - The document is removed from the print queue.
- Properties - The properties for the document are displayed.

Also remember that permissions will play a part in what level of print management your user account has.

Connect to and manage printing to a network-based printer

A shared printer is accessible to other users on the network. A printer can be shared from its properties dialog box. Select the Sharing tab; click the button beside Share this printer, and type in a share name for the printer. The Additional Drivers button can be used to install the drivers required by other versions of Windows. The clients can then download the drivers automatically when they connect to the printer.

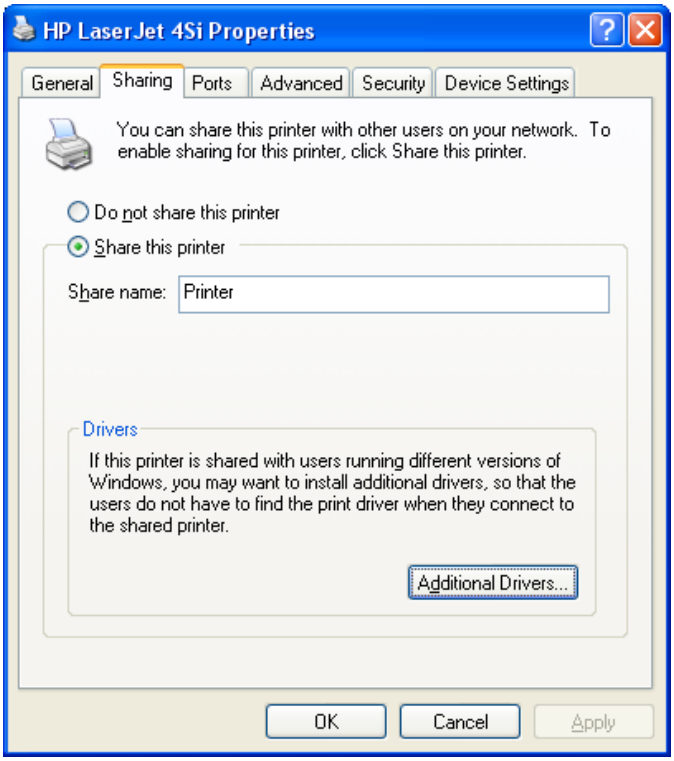

Figure: Sharing a printer

When you attach a print device to your local computer and share it, your computer is turned into a print server. Through the Printers and Faxes folder, you can configure print job notification for users that send print jobs to a Windows XP print server.

To configure print job notification:

1. Click Start and click Printers and Faxes.
2. Click the File menu and select Server Properties.
3. Click the Advanced tab from the Print Server Properties dialog box.
4. Select any of the options below for print notification.
    - Show Informational Notifications For Local Printers - You will be notified when a document has been printed on a print device attached to the local computer.
    - Show Informational Notifications For Network Printers - You will be notified when a document has been printed on a print device attached to a remote computer.
    - Notify When Remote Documents Are Printed - A message will be sent to the user who sent the print job to the print device attached to this print server. This option is for pre-Windows 2000 clients.
    - Notify Computer, Not User, When Remote Documents Are Printed - A message will be sent to the computer from which the print job was sent. This option is for pre-Windows 2000 clients.
5. Once you have selected the appropriate print notification options, click OK.

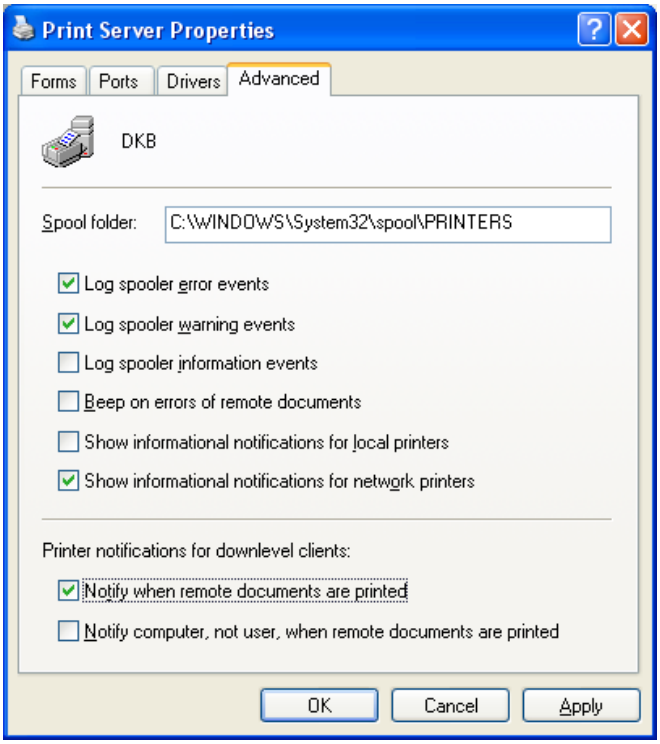

Figure: Configuring Print Job Notification

Publish a Printer in Active Directory

If you attach a printer to a computer that is a member of a domain, you can share and publish that printer in Active Directory for others to access. In order for a printer to be published in Active Directory, it must first be shared. By publishing the printer, it becomes searchable based on its attributes such as features and location. This can enable users to, for example, search for printers located on the second floor of their building. Keep in mind though; a shared printer does not need to be published in order to make it accessible to other users. They can easily connect to it using the Net Use command.

In Windows XP, you can share and publish a printer using the steps listed below:

1. Click Start and click Printers and Faxes.
2. Right-click the appropriate printer and click Properties.
3. Click the Sharing tab.
4. Click Share This Printer and type in a descriptive share name.
5. Select the List In The Directory check box.
6. Click OK.

Manage and troubleshoot access to and synchronization of offline files

Answer end-user questions related to configuring and synchronizing offline files

Network files can be made available to users when they are working offline by storing copies of the shared files on the users' computers. This is ideal for users with portable computers who need access to network files when they are disconnected from the network. Through synchronization, any changes made to offline copies of the files can be synchronized with the network copy when the computer is reconnected.

By default, the offline files feature is enabled in Windows XP. If it has been disabled at some point, it can be re-enabled using the Offline Files tab from the Folder Options dialog box. Verify that there is a check beside the Enable Offline Files option.

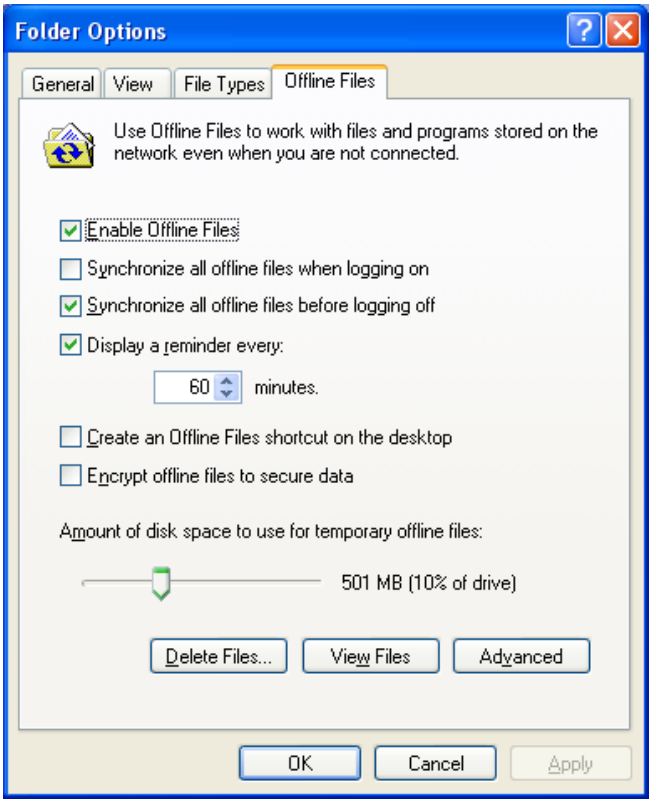

Figure: Enabling offline files

Configure and troubleshoot offline files

Once the Offline Files feature has been enabled, you need to configure a folder or file to be made available offline. Open My Computer and double-click the network drive that contains the folder or file you want to make available offline. From the File menu, click the Make Available Offline option.

Permissions applied to network files and folders remain the same when you are working offline. For example, if a user has been assigned read permission to a network file, the user will have read-only permission when working with that file offline.

Configure and troubleshoot offline file synchronization

By default, Windows XP will synchronize offline files before a user logs off the computer. Using the Offline Files tab of the Folder Options dialog box, you can configure offline files to also be synchronized when logging on to the computer.

Using the Synchronization Manager, you can configure what offline files should be synchronized when a network connection becomes active. Click Start, point to All Programs, Accessories, and click Synchronize. Click the Setup button at the bottom of the Items To Synchronize dialog box. The Synchronization Settings allow you to select what information should be synchronized for each network connection configured on a computer.

Synchronization Settings can be further customized using the On Idle and the Schedule tabs. Offline files can be synchronized when a computer has been idle for a specific amount of time. Synchronization can also take place based on a pre-configured schedule.

Configuring and Troubleshooting Hardware Devices and Drivers

Configure and troubleshoot storage devices

Answer end-user questions related to configuring hard disks and partitions or volumes

Windows XP supports two different types of disks: basic disks and dynamic disks. Windows 2000 introduced the concept of dynamic disks. It allows you to use basic disks or convert to dynamic to take advantage of additional features.

Windows 2000 and later versions of Windows support both basic and dynamic disks. Basic disks are supported by all versions of Windows including MS-DOS and Windows NT. A basic disk supports the following:

- Primary partitions
- Extended partitions
- Logical drives

A basic disk also supports different types of Redundant Array of Independent Disks (RAID) including volume sets, stripe sets, mirror sets, and stripe sets with parity.

Once your disk has been converted to dynamic, partitions will no longer be used. Instead, dynamic disks use volumes. A dynamic disk supports the following types of volumes:

- Simple volumes
- Spanned volumes
- Mirrored volumes
- Striped volumes
- RAID-5 volumes

Windows XP does not support mirrored volumes or RAID-5 volumes. However, you can use the Disk Management console on a computer running Windows XP to create a mirrored or RAID-5 volume on a remote computer that can support these volume types.

Many people want to know why they should convert to dynamic. Dynamic disks support additional features such as:

- Disk and volume management tasks can be performed without having to restart the computer afterwards.
- You can create volumes that span multiple disks. These are referred to as spanned volumes.
- You can extend a simple or spanned volume.
- Dynamic disks support a large number (up to 2000) of volumes.
- Dynamic disks do not use a Master Boot Record (MBR). Disk layout information is stored on the last 1 MB of the disk.

It is a relatively simple process to convert from basic to dynamic. You can do so through the Computer Management console as outlined below. However, keep the following points in mind before you proceed:

- There must be at least 1 MB of free space on the disk you are converting.
- You will not lose any data by converting to a dynamic disk.
- Dynamic disks are not supported by mobile computers.
- Pre-Windows 2000 operating systems do not support dynamic disks.
- External disks, such as drives connected by USB, cannot be converted to dynamic disks.
- Unless you require a feature only supported by dynamic disks, it is better to leave disks as basic.

With these points in mind, you can convert to a dynamic disk as outlined below. When you first install Windows 2000/XP Professional and Windows Server 2003, all disks are initialized as basic. You then have the option of converting to dynamic without losing any of your data.

1. Right-click My Computer and click Manage.
2. Click Disk Management.
3. In the right pane, right-click the disk you want to convert and click Convert To Dynamic Disk.
4. Place a check beside the disk you want to convert. Click OK.
5. Click Convert.
6. Click Yes.
7. Click OK.

Manage and troubleshoot disk partitioning

You can create a new simple volume or spanned volume by completing the steps below:

1. Open the Disk Management console.
2. Right-click unallocated space on the dynamic disk and click New Volume. Alternatively, click unallocated space on one of the dynamic disks to create a spanned volume. Click Next.
3. Select the type of volume to create: Simple, Spanned, or Striped. Click Next.
4. Verify that the disk or disks on which you want the volume are selected and type in the size of the volume. Click Next.
5. Assign a drive letter to the volume and click Next.
6. Specify the formatting options. If you choose to format the partition, type in a name for the volume in the Volume Label field and select the file system you want to use. Click Next.
7. Click Finish.

One of the advantages of converting to a dynamic disk is that you can extend a simple volume. This means if you have additional free space on a different disk, you can use it to extend an existing simple volume without losing any data.

Before you attempt to extend a simple volume, there are a few things you need to keep in mind. A primary partition becomes a simple volume when the disk is converted from basic to dynamic. However, if the simple volume was created before the disk was converted to dynamic, it cannot be extended. A simple volume can only be extended if the simple volume was created after the disk was converted to dynamic. A simple volume that was originally a primary partition cannot be extended and you cannot extend the system or boot volume.

To extend a simple volume:

1. Open the Disk Management console.
2. Right-click the simple or spanned volume that you want to extend. Click Extend Volume.
3. Click Next. If necessary, select the disk that the volume will be extended to and click Add.
4. Specify the amount of space to add to the volume. Click Next.
5. Click Finish.

You can use the Disk Management console in Windows XP to change the drive letter that is assigned to a partition or volume. You can assign letters C through Z to the volumes on your hard drives. Letters A and B are reserved for the floppy disk drives in your computer.

Before you start changing the drive letters, you need to keep two important points in mind: First of all, the Disk Management console cannot be used to change the drive letter assigned to the system or boot volume. Second, some MS-DOS programs refer to specific drive letters for environmental variables. Therefore, altering the drive letters may cause some of these programs to not function correctly.

With those points in mind, you can use the steps listed below to change the drive letter assigned to a volume:

1. Open the Computer Management console.
2. Click Disk Management (Local) in the left pane.
3. Right-click the appropriate volume and select Change Drive Letter And Paths.
4. Click Change.

5. Click Assign The Following Drive Letter and click the drive letter you want to use.
6. Click OK.
7. Click Yes to confirm your actions.

The new drive letter you selected will now be assigned to the volume.

If you convert to a dynamic disk, you can move disks between computers, but additional steps are required. After a disk has been physically moved between computers, its status will be marked as foreign on the destination computer. You will be unable to access any data on the disk until it is imported into the computer's system configuration.

Once a dynamic disk has been moved from one computer to another, you can use the steps below to import it. The steps below assume that you have already physically added the foreign disk to the computer.

1. Click Start and click Run.
2. Type mmc and click OK.
3. Click Add/Remove Snap-in from the File menu.
4. Click Add. Select Disk Management, click Add then Finish, and click Close.
5. Click OK.
6. Click Disk Management (Local) in the left pane.
7. From the Action menu, click Rescan Disks.
8. Right-click the disk marked as Foreign and click Import Foreign Disks.
9. Follow the onscreen instructions to complete the process.

You should now be able to access the data that is stored on the new disk.

Disk Problems

The Disk Management console will display the status of each disk and volume on a computer. You can use the status messages to help troubleshoot disk problems. Status messages can include any of the following:

- **Online -** This message indicates that the disk is accessible and there are no problems.
- **Online (errors) -** The disk is accessible; however, I/O errors have been detected.
- **Offline** - This disk is not accessible. The disk may be powered off, disconnected, or corrupt.
- **Unreadable -** This disk is not accessible. The status message may be caused by a hardware failure, a corrupt disk, or I/O errors.
- **Foreign** - The disk has been moved to this computer from another computer running Windows 2000 or Windows XP. The disk must be imported using the Import Foreign Disk option.
- **Unrecognized** - The signature on the disk is not supported by Disk Management.

Windows XP includes other tools that can be used to diagnose and resolve disk problems. You can use the Add Hardware applet within the Control Panel and you can use Device Manager. The properties dialog box for the specific hardware device within Device Manager will provide information about the status of the device. The CheckDisk (chkdsk.exe) tool is used to check for file system errors and bad sector. To scan a disk for errors, open My Computer, right-click the appropriate disk and click Properties. From the Tools tab, click the Check Now button under Error-checking.

Device Manager

Device Manager provides a graphical view of the hardware that is currently installed on the computer. The device drivers and resources associated with that hardware are listed in the properties of each device.

Device Manager is used to maintain, configure, and troubleshoot the devices physically connected to the computer system.

The following items outline some of the available functionalities:

- Determine if the hardware is working properly on the computer.
- Change hardware configuration settings.
- Identify the device drivers that are loaded for each device and obtain information about each device driver.
- Change advanced settings and properties for devices.
- Install updated device drivers.
- Disable, enable, and uninstall devices.
- Reinstall the previous version of a driver with the Roll back feature.
- Identify device conflicts and manually configure resource settings.
- Print a summary of the devices that are configured on your computer.

The installation of device drivers may vary between manufacturers. Typically, if the device is Plug and Play, plug the device into your computer and the device installation should be automatically initiated. You can also use the Add Hardware Wizard to install devices.

Sometimes updating a device driver can result in additional problems. Device Manager can be used to revert back to the previous driver. You can revert back to the previous driver by using the Roll Back Driver button available on the Driver tab from the device's properties window.

To use the Roll Back feature with Windows XP, open the Device Manager and follow these steps:

1. Right-click the device for which you want to re-install the previous version of the driver and click Properties.
2. Click the Drivers tab.
3. Click the Roll Back Driver button.

Driver Signing

When it comes to device drivers, you should also be familiar with driver signing options. Microsoft introduced driver signing because the majority of blue screens were caused by flakey drivers developed by third-parties. Driver signing is a process Microsoft uses to validate that a driver isn't likely to crash. Using signed drivers is more about stability than compatibility, as Windows XP won't install incompatible drivers, but it will install unstable drivers. Driver signing options are configured using the Hardware tab from the System Properties dialog box. Driver signing options include:

- Ignore - All drivers, signed or unsigned, can be installed.
- Warn (default) - Prompts the user whether or not to install an unsigned driver.
- Block - Unsigned drivers cannot be installed.

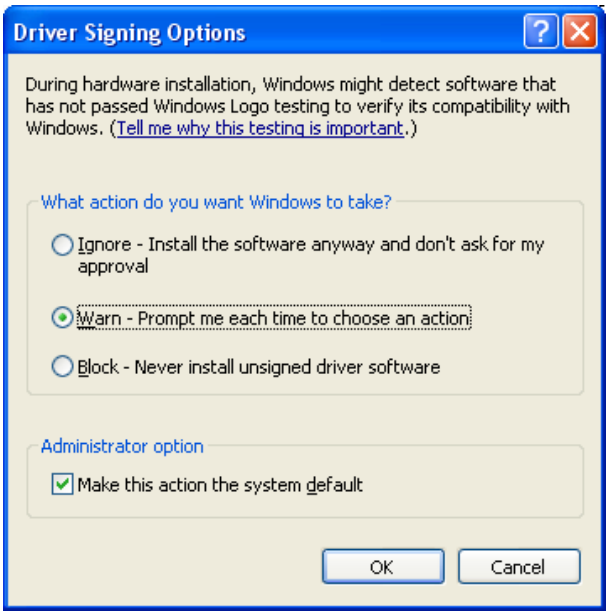

Figure: Configuring driver signing options

Hardware Profiles

A hardware profile will tell Windows which devices to use when your computer starts up. Hardware Profiles are typically considered to be an outdated technology because Windows XP automatically detects when hardware is added or removed. The only reason to use hardware profiles is if you want Windows XP to ignore hardware that is physically attached at certain times.

You can create a hardware profile using the steps outlined below:

1. Right-click My Computer and then click Properties.
2. From the Hardware tab, click the Hardware Profiles button.
3. Under the list of available hardware profiles, select Docked Profile or Undocked Profile and click Copy.
4. Type in a new name for the profile and click OK.
5. Click OK.

When you reboot your system, Windows will prompt you to select which hardware profile you want to use.

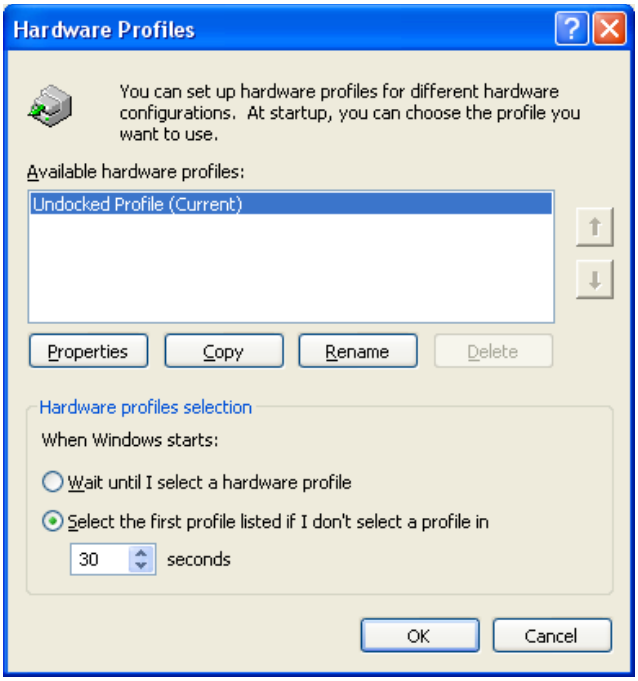

Figure: Creating a hardware Profile

Answer end-user questions related to optical drives such as CD-ROM, CD-RW, DVD, and DVD-R

CD-R and CD-RW drives have become common components of desktop computers. Windows XP allows users to write information to CD without having to install additional software. Data can be copied to a CD using the following procedure:

1. Insert a writable CD into the CD burner/recorder.
2. Within My Computer, select the data you want to write to CD.
3. Under the list of tasks, select Copy This File, Copy This Folder, or Copy the Selected items.
4. From the dialog box that appears, click the CD recording drive and click Copy.
5. Double-click the CD recording drive within My Computer.
6. Under the list of tasks, select Write These Files To The CD.

If you are using a CD-RW, you can also erase files on a CD. You must erase all files. Users do not have the option of erasing individual files. CD-R disks are not erasable.

Administrators can prevent users from burning CDs by editing the local policy. Within the Group Policy Editor (Click Start, click Run, and type gpedit.msc), expand User Configuration | Administrative Templates | Windows Components | Windows Explorer, and double-click the Remove CD Burning Features setting in the details pane. Click Enabled and click OK. Once this setting is enabled and the Group Policy is applied, all CD burning features will be removed from Windows Explorer.

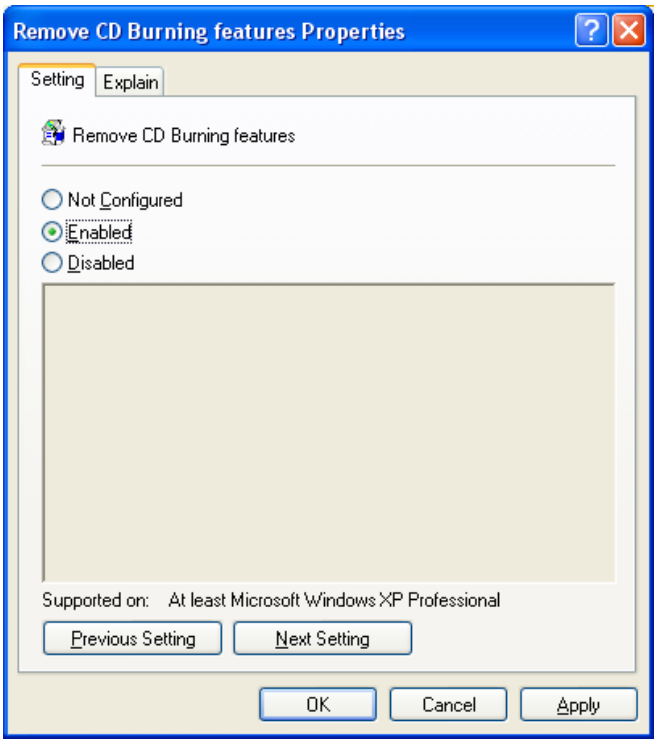

Figure: Disabling CD Burning Features

If a user is having problems copying data to a CD-R or CD-RW, you can use the following points to assist in troubleshooting.

- Verify that the CD and the CD drive are clean.
- Check that there is enough space on the CD.
- Check that there is enough disk space to store the temporary files being written to the CD.
    - Use the Disk Cleanup Wizard to free up disk space.
    - Move the temporary storage area to a partition with more free space.
- Verify that a CD-RW is being used if a user is trying to append or erase files to a CD.
- Disable any screensavers that may be interrupting the writing process.

Configure and troubleshoot removable storage devices such as pen drives, flash drives, and memory cards

Windows XP supports storage devices other than just hard drives. The benefit is that users can store data on devices such as pen drives, flash drives, and memory cards. The disadvantage is that it can create more troubleshooting.

There are several points that a Desktop Support Technician should keep in mind when working with removable storage devices.

- If removable storage devices are ejected prematurely, users may experience problems and receive an error message. Data on the device may also be lost.
- Administrators can control which users are allowed to format and eject removable devices.
    - Within the local policy expand Computer Configuration | Windows Settings | Security Settings | Local Policies | Security Options and double-click the Devices: Allowed to Format and Eject Removable Objects.
    - By default, only administrators are granted this right.
- Verify that the removable storage device is supported by Windows XP.
- Use Device Manager to ensure that the correct device drivers are installed.
- Use the Windows Event Viewer to locate any removable storage related error messages.

Configure and troubleshoot display devices

Configure display devices and display settings

- Desktop settings can be configured through the Display properties dialog box.
    - Open the Display applet within the Control Panel.
    - Right-click a blank area of the desktop and select Properties.
- The Desktop applet can be used to configure various settings.
    - Themes - Used to change the theme displayed on the desktop.
    - Desktop - Used to change the background displayed on the desktop.
    - Screensaver - Used to change the screensaver and implement a password-protected screensaver.
    - Appearance - Used to increase the font size and change the color schemes.
    - Settings - Used to configure multiple monitors, advanced settings, and troubleshoot display problems.

Screensavers can serve a much more important purpose other than providing us with a few minutes of visual pleasure. Enabling a screensaver can actually increase the security on your computer. You can configure a screensaver to start when a computer has been idle for a specific amount of time (for example, after 5 minutes). By password protecting the screensaver, the computer will be locked when the screensaver starts. In order to return to the desktop and resume working, the user will need to supply the correct password. Once a password-protected screensaver has been enabled, a user can walk away from the computer knowing their folders and files have some level of protection. In Windows XP, you can use the steps outlined below to enable a password-protected screensaver.

1. Right-click your desktop and click Properties.
2. From the Display Properties dialog box, select the Screensaver tab.
3. Use the drop down arrow to select your screensaver of choice.
4. Change the Wait value to specify how long the computer can remain idle before the screensaver is started.
5. Select the On Resume, Password Protect option. If you do not select this option, any activity will cause the desktop to appear.

Configure and troubleshoot Advanced Configuration Power Interface (ACPI)

Configure and troubleshoot system standby and hibernate settings

- Advanced Power Management (APM)
  - Windows will disable APM if the system is not compatible
- Advanced Configuration and Power Interface (ACPI)
  - APM cannot be used if ACPI is currently in use
- Different modes to conserve battery power on mobile computers
  - Suspend mode
    - Uses minimal power
  - Hibernate mode
    - System is powered down and restarted
    - System is in the same state as when shut down

Configuring and Troubleshooting the Desktop and User Environments

Configure the user environment

Configure and troubleshoot task and toolbar settings

The Start Menu and Taskbar are two components found on the Windows desktop. The Start Menu (opened by clicking the Start button on the desktop) displays a menu that can be used to gain quick access to different areas or different programs installed on a computer. For example, you can launch a favorite program or open the Control Panel.

By default, the Taskbar is located along the bottom of the desktop. The Taskbar serves many purposes, one of which is fast switching between open programs. Each program that is currently running has a button on the taskbar that makes it easy for a user to switch between programs. The Taskbar also contains the Start button, the Quick launch area, and the notification area.

Windows XP allows you to customize both the Taskbar and the Start Menu to suit specific needs. In terms of troubleshooting, it will make it easier to assist end-users with problems if you have a general understanding of the different options for customizing both components.

You can begin customizing the Taskbar by right-clicking on the Start button and clicking the Properties option. This opens the Taskbar and Start Menu Properties dialog box. Using the settings available from the Taskbar tab, you can configure the appearance of the Taskbar and the Notification area.

The table below summarizes the different options available for customizing the appearance of the Taskbar.

Option	Description
Lock The Taskbar	The taskbar is locked in its current position on the desktop so it cannot be moved.
Auto-hide The Taskbar	The taskbar will be hidden on the desktop. The taskbar will reappear when you point to the area of the desktop where the taskbar is located.
Keep The Taskbar On Top Of Other Windows	Ensures the taskbar is always visible.
Group Similar Taskbar Buttons	If the taskbar becomes too crowded with buttons, buttons for the same program are combined into a single button.
Show Quick Launch	The quick launch bar is displayed on the taskbar.

The remaining options are used to configure the Notification area of the taskbar (this is the area of the taskbar that displays the clock). If you do not want the clock displayed, simply clear the option to Show the clock. You can also keep the Notification area less cluttered by having inactive icons hidden (these are icons you have not recently clicked). Once the Hide inactive icons option is selected, you can use the Customize button to specify which items you want hidden when inactive.

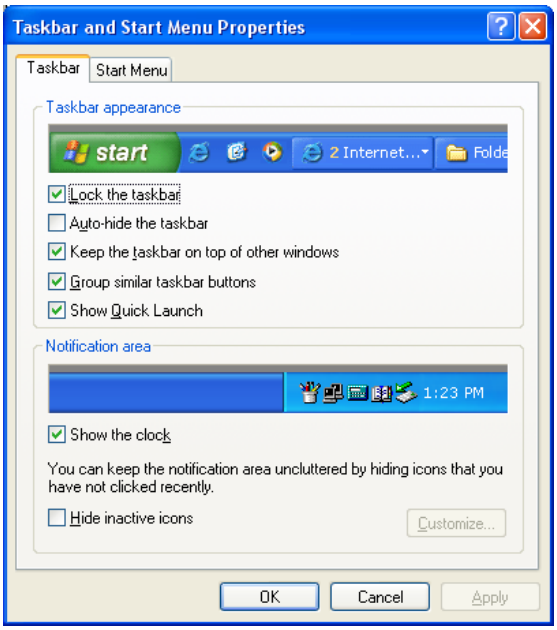

Figure: Configuring the taskbar

The Start Menu in Windows XP is divided into distinct sections. The left side of the Start Menu consists of pinned programs, recently used programs, and All Programs. Pinned programs must be manually added to the Start Menu. Your default email program and web browser will always appear, and additional programs can be added. Beneath the pinned programs are the recently used programs. The programs displayed here will change, as the most recently used programs will replace those that have not been used. The All Programs option contains a submenu displaying all the programs currently installed on a computer. A program can be pinned to the Start Menu by right-clicking the specific program and selecting Pin to Start Menu. The program will appear as a pinned program for the user who is currently logged on to the computer.

Using the Start Menu tab from the Taskbar and Start Menu Properties dialog box, you can customize the appearance and behavior of the Start Menu. Once you click the Customize button, the Customize Start Menu dialog box appears.

Figure: Configuring the StartMenu

Using the General tab, you can change the size of the icons for programs displayed on the Start Menu. You can also change the number of programs that appear on the frequently used list (these are the programs located below the separator line on the Start Menu), and specify which programs are used to access the Internet and Email. For example, if you use Internet Explorer for web access, you will more than likely want this program displayed on the Start Menu as opposed to a web browser that you use less frequently.

Selecting the Advanced tab presents you with a number of other options that can be used to customize the Start Menu. The table below summarizes the various settings available.

Option	Description
Open Submenus When I Pause On Them With My Mouse	If the item contains a submenu, it is immediately displayed when pointed to.
Highlight Newly Installed Programs	New programs are highlighted in a different color on the All Programs list.
Start Menu Items	Allows you to specify which items should be displayed on the Start Menu.
List My Most Recently Opened Documents	If this option is selected, an item is displayed on the Start Menu called My Recent Documents. Any documents recently opened are displayed on this list.

If you customize the Start Menu using the Taskbar and Start Menu dialog box, the changes will only be applied to the user that is currently logged on to the computer.

If a computer is shared between multiple users, you can prevent them from making certain changes on the computer. Some people may find it a nuisance to leave their computer only to come back and find that it now looks completely different, or even worse; find that your computer is not operating as it should.

One of the things you can do is restrict access to the Taskbar and Start Menu settings. Users will be unable to open the Taskbar Properties dialog box and make changes to the existing settings. You can accomplish this by following the steps listed below.

1. Click Start and click Run.
2. Type gpedit.msc and click OK.
3. Expand User Configuration | Administrative Templates | Start Menu and Taskbar.
4. In the details pane, double-click Prevent Changes To The Taskbar And Start Menu Settings.
5. Click Enabled.
6. Click OK.
7. Close the Group Policy editor.

Now when a user attempts to make changes to the Start Menu and Taskbar by right-clicking the taskbar and clicking Properties, a message will appear indicating that the action cannot be performed.

Configure and troubleshoot accessibility options

Windows XP includes different accessibility features so that people with disabilities can also use the operating system. You can find the Accessibility Options applet within the Control Panel. The Accessibility Options tabs include: Keyboard, Sound, Display, Mouse, and General.

From the Keyboard tab, you can configure the following:

- StickyKeys
  - Users only need to press one key at a time for keystrokes.
- FilterKeys
  - Brief or repeated keystrokes are ignored.
- ToggleKeys
  - A sound is emitted when a locking key is pressed.

Windows XP can accommodate users with hearing impairments. You can configure the sound-related accessibility features within the Control Panel. Simply double-click the Accessibility Options applet and select the Sound tab.

Windows XP includes different features that make it easier for people with vision impairments to use the operating system. One such feature is known as the Magnifier. You can use this feature to enlarge the screen so it is easier to read. The Magnifier works by magnifying a portion of the screen as it is being displayed. The feature is intended for those users who have slight vision problems.

After a mouse has been installed on a computer, you can adjust certain settings using the Mouse tab of the Accessibility Options dialog box. It allows you to control such settings at the speed and acceleration of the mouse pointer.

Configure and troubleshoot fast-user switching

Microsoft has recognized the fact that a single computer is often shared between multiple users. Windows XP Home and Professional editions make it easier for users to share a computer using the Fast User Switching feature.

This feature allows more than one user to log on simultaneously at a single computer. For example, if you are currently logged on to a computer, another user can log on to check their email without you having to close your open programs and log off. Once the user is finished, you can return to your session where all your programs will still be running.

By default, Fast User Switching is enabled in Windows XP Home and Windows XP Professional editions (only if there is 64 MB of RAM or more). However, if you are running Windows XP Professional and you are part of a domain, this feature is disabled.

You can enable or disable the feature using the following steps:

1. Click Start, click Control Panel, and click User Accounts.
2. Click the option to Change The Way Users Log On Or Off.
3. Make sure Use The Welcome screen is selected.
4. Click Use The Fast User Switching check box. Click the Apply Options button.

Configure support for multiple languages or multiple locations

Configure and troubleshoot regional and language settings

Regional Settings affect how Windows XP and different programs display information such as numbers, currency, time, and date. Regional settings can be changed using the Regional and Languages Options applet within the Control Panel.

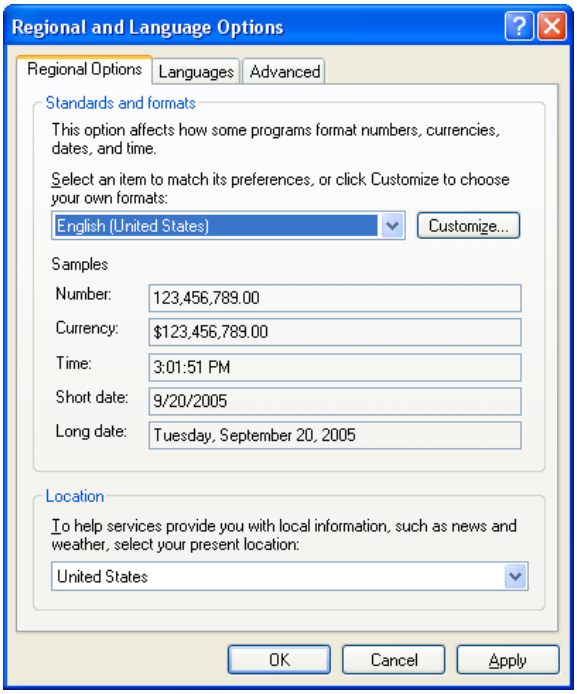

Figure: Configuring regional and language settings

Using the Regional Options tab, you can select your specific local, such as English (United States), to determine how certain items will be formatted. Using the Customize button, you can manually configure how the different regional options will be displayed.

The Languages tab allows you to configure the input languages. These are the languages in which text can be entered and displayed. You can also add support for additional languages.

Troubleshoot security settings and local security policy

Identify end-user issues caused by local security policies such as Local Security Settings and Security Configuration and Analysis

Windows XP includes a local security policy that can be used to configure security settings on a local computer. You can access the security settings by opening the Local Security Policy applet within the Control Panel.

- Security settings include:
  - Account Policies
    - Password Policy
    - Account Lockout Policy

    - Local Policies
        - Audit Policy
        - User Right Assignment
        - Security Options
    - Public Key Policies
        - Encrypting File System
    - Software Restriction Policies
        - Security Levels
        - Additional Rules
    - IPSec Policies
- Auditing can be enabled through the local security policy
- Enable auditing to track access to network resources
    - Enable an audit policy
    - Specify which resources to audit
- Use the Security Templates console to create custom templates
- Security templates
    - Deploy security settings
    - Audit existing security settings
- Security Configuration and Analysis can be used to compare current security settings against those in a security template to identify discrepancies

Identify end-user issues caused by network security policies such as Resultant Set of Policy (RSoP) and Group Policy

Security policy settings can be applied locally through the local security policy. If the computer is a member of the domain, security settings can also be applied through a domain-based **group policy object** (GPO).

Within an Active Directory domain, a GPO can be applied at the site, domain, and **Organization Unit** (OU) level. The settings applied locally are overwritten by those applied through a GPO. This means a computer and/or user can be affected by multiple policies. You can troubleshoot security settings using Resultant Set of Policy (RSoP).

The Resultant Set of Policy (RSoP) tool helps administrators troubleshoot, plan, and monitor group policy settings. It allows administrators to see the effective policy settings and determine the effect of policy setting changes.

Resultant Set of Policy can be used in two different modes: Planning mode and Logging mode. In planning mode, you can see the effect that certain policy settings will have. You can use RSoP in planning mode using the following steps:

1. Click Start, click Run, type mmc and click OK.
2. Click File and select Add/Remove Programs.
3. From the Add/Remove Snap-in dialog box, click Add.

4. From the Add Standalone Snap-in window, scroll through the list of available snap-ins and select Resultant Set of Policy. Click Add. Click Close. Click OK.
5. Select Generate RsoP Data from the Action menu. This launches the Resultant Set of Policy Wizard. Click Next.
6. From the Mode Selection page (which appears only if the computer is a member of an Active Directory domain), you can select the mode you want to use. Select Planning Mode. Click Next.
7. From the User And Computer Selection page, you can choose the user account, computer, or container that you want to simulate the settings for.
8. Under Computer Information, select Computer and click Browse. Locate your computer and click OK. Click Next.
9. From the Advanced Simulation Options page, you can select any optional parameters. Click Next.
10. From the Alternate Active Directory Paths page, you can configure an Active Directory path other than the current one. Click Next.
11. Using the Computer Security Groups, you can simulate the results of the user or computer belonging to different security groups. Click Next.
12. Review the Summary Of Selections and click Next. Click Finish.
13. The results of the query are displayed in the RsoP console.

Logging mode queries are performed to view all the IPSec policies that are currently assigned to a computer. This is useful when a computer is affected by multiple policies. The results of the query will display which policies a computer is affected by, the precedence of each policy, and the settings for the IPSec policy that is being applied to the computer. You can run RSoP in Logging mode using the following steps:

1. Open the Resultant Set of Policy snap-in.
2. From the Action menu, select Generate RsoP Data. This launches the Resultant Set of Policy Wizard. Click Next.
3. From the Mode Selection dialog box, you can select the mode you want to use if your computer is a member of an Active Directory domain. Leave the default mode (Logging Mode) selected. Click Next.
4. The next dialog box allows you to select the computer for which you want to display IPSec policy settings. Select This Computer, if not already selected. Click Next.
5. From the User Selection window, you can specify what settings you want to display. You can display results for the current user logged on, a specific user, or display computer settings only. Leave the default option of Current user selected. Click Next.
6. Review the Summary of Selections and click Next.
7. Once the wizard has completed gathering the required information, click Finish.
8. You can view the IPSec policy settings by navigating to the User Configuration, Windows Settings, Security Settings, and IP Security Policies on Local Computer container.

Configure and troubleshoot local user and group accounts

Answer end-user questions related to user accounts

Local user accounts are local to a specific computer. A local user account gives a user the ability to log on to a local computer and access local resources only. Once a local user account is created, it is stored within the local security database only. When you log on with a local account, the local computer authenticates the log on request using its local security database.

Domain user accounts are stored as objects within Active Directory as replicated between domain controllers in the same domain. A domain user account gives a user the ability to log on to a domain and access resources for which the account has been granted access. They provide users with a single sign-on, meaning they only need to log on once to access network resources.

During the logon process, a user provides a valid name and password. A domain controller within the domain uses the information provided by the user to authenticate them and generate an access token. An access token is similar to a form of identification that you might present to identify yourself. The access token then identifies the user to other computers when they attempt to access resources.

The third type of user accounts are those that are built-in. Once you install Windows XP, several user accounts are automatically created. These include the Administrator, Guest, and HelpAssistant accounts. Logging on with the Administrator account gives you the right to administer the computer. The Guest account is designed mainly for those users requiring occasional access to the computer. The HelpAssistant account is installed with a Remote Assistance session. By default, both the Guest and HelpAssistant account are disabled.

Configure and troubleshoot local user accounts

Windows XP makes it simple to create user accounts, so each person who accesses the computer can have their own logon and personalized settings. To create a new user account, open the User Accounts applet found within the Control Panel. From the list of tasks, select Create A New Account. Windows XP will then walk you through the process of creating the account.

While you create the account, you will be given the option of what type of account it should be (a computer administrator or an account with limited permissions). It is generally a good idea to create limited accounts for regular users. This reduces the chance of someone unknowingly causing harm to the computer.

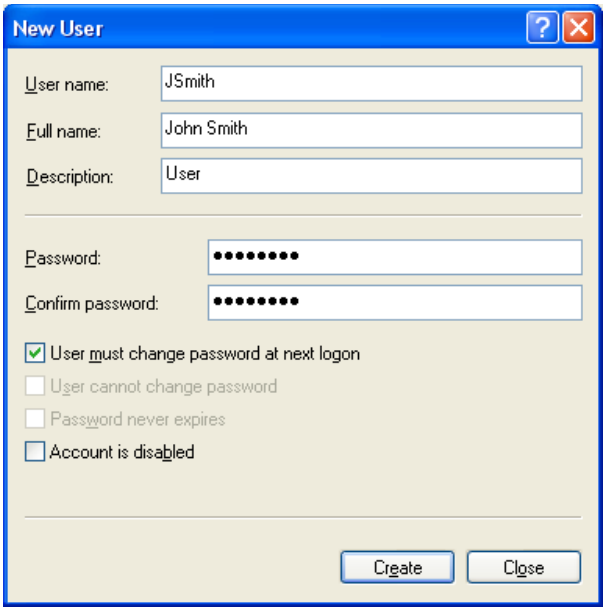

Figure: Creating a new user account

Answer end-user questions related to local group accounts

Local groups are created to assign rights and permissions to resource on a local computer only. For example, if you create a local group on a computer, that group can only be used on that computer; you cannot use the group to assign permissions to resources on another computer.

Configure and troubleshoot local group accounts

Local group accounts can be created using the Local Users and Groups within the Computer Management console. Once you select the Groups folder, the right pane will display the built-in groups created during the installation of Windows XP as well as any groups that have been manually created. The table below describes the default local groups included with Windows XP.

Built-in Local Groups	Description
Administrators	Members of this group can perform all administrative tasks on the computer.
Backup Operators	Members of this group can backup and restore data on the computer.
Power Users	Members of this group have the ability to perform most administrative tasks on the local computer.
Remote Desktop Users	Members of this group can remotely logon to the computer.
Replicator	This group is used by the File replication Service.

Users	Members of this group have limited privileges on the computer.
Network Configuration Operators	Members of this group can make changes to the TCO/IP settings in the computer.
HelpServicesGroup	This group is for the help and Support Center.

A group can be created by selecting the Groups folder and clicking the New Group item from the Action menu. From the New Group dialog box, type in the group name and an optional description. You can use the Add button to select which user accounts will be members of the group. The group can be used to grant rights and permissions to its members.

Troubleshoot system startup and user logon problems

Troubleshoot system startup problems

A Desktop Support Technician must know the different options available to recover a computer in the event of failure. One such option is **Automated System Recovery,** or ASR.

First of all, you need to know how to create the ASR backup set. You can create it by following the steps listed below:

1. Click Start, point to All Programs, Accessories, System Tools, and click Backup.
2. Click the Automated System Recovery Wizard button.
3. Click Next.
4. Select a destination for the backup and a filename, and then click Next.
5. Click Finish.
6. Insert a blank, formatted floppy disk.

The information that is stored on the ASR floppy always includes the following:

- Registry
- COM+ Class Registration database
- Boot files, including system files
- System files that are under Windows File Protection

You also need to know what to do with the ASR floppy in the event of computer failure. By following the steps below, you can use the ASR backup and floppy disk to restore the system to the state it was when these components were created.

1. Insert the Windows XP installation CD-ROM. If prompted, press any key to boot from the CD-ROM.
2. When prompted, press F2 to run Automated System Recovery (ASR).
3. Insert the ASR floppy disk.

4. Once the computer reboots, the Automated System Recovery Wizard will start.
5. Confirm the location of the disk backup file.
6. Once the process is complete, verify that all data and settings have been restored.

Other options for troubleshooting startup issues include using the different boot menu options and the Recovery Console.

- Safe mode - F8 at system startup
  - Enable Boot Logging
  - Enable VGA Mode
  - Last Known Good Configuration
  - Recovery Console
  - Debugging Mode
- Recovery Console can be installed on the local computer

Troubleshoot local user logon issues

- Verify that a user is logging on with the correct username and password.
- Check to see that the user has an account on the local computer.
- Account lockout policy determines how many failed logon attempts before user account is locked out. This setting can prevent users from logging on.
  - Account is locked for a specific amount of time or until it is unlocked by an administrator
  - Account policy settings
    - Account lockout duration
    - Account lockout threshold
    - Reset account lockout after
- Password policy settings
  - Enforce password history
  - Maximum password age

Troubleshoot domain user logon issues

- Verify user is logging on with the correct credentials
- Valid user account required to log on to a domain
- User cannot log on if user account has been disabled

Monitor and analyze system performance

Use Task Manager to view and troubleshoot system performance

There are now four tabs within the Task Manager window instead of two as seen with NT and the three with Windows 2000. The Applications tab serves to display all of the active applications on the system. Services and application-spawned processes will not appear with this tab. The Processes tab, however, will display all processes running on the server – applications, processes, and services.

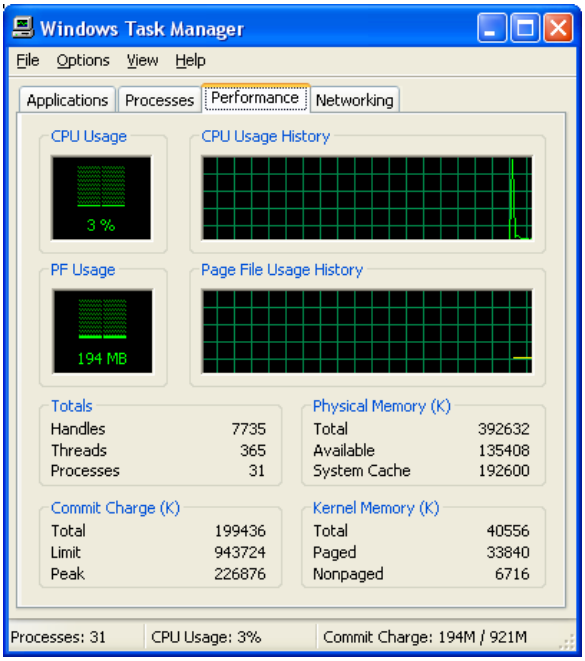

Figure: Windows XP Task Manager

From within either the Applications or the Processes tab, you have the ability to stop an entry. This doesn't mean that you can always do so successfully. Many applications will spawn multiple processes that are either system-protected, or so interrelated that stopping an application or process is impossible to do without compromising system integrity. When this happens, you will either be presented with a message indicating that the app/process cannot be stopped, or a cycle of messages that amount to the same thing. There are two new Windows XP commands that can be used to potentially wrestle a service or process to the ground: SC and TASKKILL. SC is specifically designed to control services, and incidentally, it can be used to create a service from a program. In this situation, you might use SC to stop a service, or unload it altogether. The TASKKILL command is used as a command-equivalent for the processes tab within Task Manager. It can sometimes end a process that stubbornly hangs on within the GUI program.

One additional feature that is available with Windows XP is the ability to right-click on an application listed on the Application tab and click Go To Process. This will switch to the Processes tab, with the associated process highlighted. It will not, however, display all associated processes.

You can identify the processes that are using CPU time by clicking the Processes tab and sorting by CPU. You can also change the priority of processes so that a long-running process does not slow down the computer.

The Performance tab is used as a quick graphical means of looking at the most important parts of the system. The graphical displays for CPU utilization closely resemble Performance Monitor's System Monitor. You do not have the ability to add objects and counters, but then again, you do not have to worry about associated system overhead either, since the Performance tab is always available. The Performance tab can be used as a constant display that will help you identify problems as they occur, such as memory leaks, or high CPU, or pagefile usage.

New to Windows XP is the Networking tab that will display network utilization for all installed network cards.

Use the Performance tool to capture system performance information

The Performance console will help you determine and deal with problems associated with a computer. The Performance console includes two components: System Monitor and Performance Logs and Alerts. System Monitor is used to monitor the real-time performance of a computer. Performance Logs and Alerts is the primary tool by which you can create baselines, document activity, and also track objects and counters over a period of time.

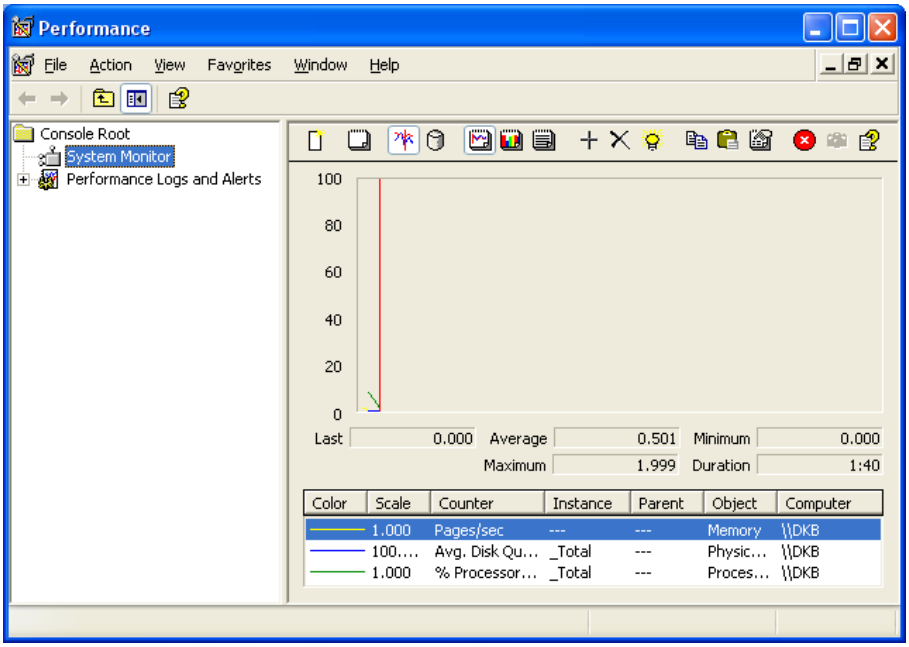

Figure: Windows XP Performance Console

A Baseline is simply a set of data that depicts the 'norm' for a particular object, event, or status. Creating a baseline is done by simply monitoring certain components, such as CPU, Memory, and Hard Disk, over a period of time when the computer is known to be healthy and functioning well. The baseline itself is then stored somewhere safe and dragged out for comparison when it becomes necessary to troubleshoot problems. Baseline information allows you to better gauge when and where your computer is functioning properly and when it is not.

Some of the common counters used to monitor computer performance and establish a baseline include:

- Memory
  - Pages/sec
  - Available bytes
- Processor
  - % Total Processor Time - A continuously high value may indicate a bottleneck
  - Processor Queue Length
- Disk
  - Logical Disk: % Free Space
  - Logical Disk: % Disk Time - Over 50% indicates a bottleneck
  - Physical Disk: Avg. Read Queue Length - Value should be lower than 2
  - Physical Disk: Avg. Write Queue Length - Value should be lower than 2
- Network
  - Network Interface: Output Queue Length
  - % network utilization

The Performance Logs and Alerts section is divided into three subsections: Counter Logs, Trace Logs, and Alerts .

- **Counter Logs**
  - Counter Logs are the logging equivalent of what you see within System Monitor.
  - Right-clicking on an empty section of the right pane will enable you to create a new log and subsequently define the logfile, its output type (text, binary, etc), and the objects/counters that the log will maintain.
  - Counters track specific events related to a given object. Unlike Windows NT, you have the option for choosing all counters within a single object, or choosing multiple counters that belong to separate objects.
  - The purpose again, is to enable you to track only the information that has the impact that you are searching for.
- **Trace Logs**
  - Trace logs track everything that the system does, but only after a specific event has occurred, such as a page fault or disk i/o.
  - These events are tracked for a specified period of time, and each triggered trace log is stored in a separate file or in a single FIFO (first in, first out) bucket.
  - Generating a new logfile for each event allows for both quick and enhanced viewing: simply looking at the number of logs generated over a period of time for a page fault might alert you that there are either paging or disk problems on the horizon.
  - Looking at the trace data itself (which must be parsed for viewing), can glean additional specific information about the system at the time that the fault occurred.

- **Alerts**
  - Alerts perform one or more tasks based upon a specific event occurrence, however, they offer more flexibility in the types of events that are available, and also the tasks that can be performed.
  - Alerts are counter-based, and are generated once a set threshold has been met.
    - It can generate an event in the Event Viewer.
    - It can send a network message to someone (usually an administrator).
    - It can run a program (any program actually) that will page or email someone with information.
  - The true value in the Alerts option lies in the fact that once a threshold has been met, it has the ability to start a Counter Log that has already been saved and configured to handle further monitoring after the event has occurred.

Using the Performance Logs and Alerts tool, you can configure administrative alerts. This way when problems occur on your computer, you can be notified of them. When you set up an administrative alert, your computer will perform a specific action when the values for the counters included in the alert indicate a problem is occurring. This is particularly useful for monitoring computers that are critical to your day-to-day operations.

You can set up administrative alerts through the Performance console using the steps outlined below:

1. Click Start and click Run.
2. Type perfmon.msc and click OK.
3. Expand Performance Logs and Alerts.
4. Right-click Alerts and click New Alert Settings.
5. Type in a name for the new alert and click OK.
6. The properties dialog box for the new alert will appear. Click the Add button to specify the counters you want monitored in the alert.
7. Click Close.
8. Highlight each counter in the list and specify the value that will trigger an administrative alert.
9. Use the Sample Data Every field to configure the sampling interval.
10. Use the Run As field to specify a different user account under which the monitoring will occur.
11. Click the Action tab.
12. Choose the actions you want to occur when the alert is triggered.
13. Use the Schedule tab to specify when to begin monitoring the counters and how long to monitor them.
14. Click OK.

Troubleshoot Network Protocols and Services

Troubleshoot TCP/IP

Answer end-user questions related to configuring TCP/IP settings

In order for packets to be routed on an IP network, every host requires a unique IP address (hosts can include workstations, servers, routers, printers, or any other device with a network interface card). The IP address is a 32-bit number represented in decimal format that identifies each host.

An IP address consists of two parts: the network ID and the host ID. The network ID is used to identify a specific network or subnet while the host ID identifies the hosts on a given network or subnet.

The network ID is used to determine if a destination host is on the local network. If the network ID of the destination host does not correspond to the network ID of the local host, the packet is forwarded to the default gateway. From there, the default gateway uses the information in its routing tables to determine which network or subnet the packet should be forwarded to.

When assigning IP addresses, each host also requires a subnet mask that determines which part of an IP address is used as the network ID and which is used to identify a host. For example, the default subnet mask for a Class C address is 255.255.255.0, which means the first three decimal places identify the network and the last decimal place identifies the host. The subnet mask is also used to determine whether the destination host is on the local subnet or a remote subnet. The subnet mask of the local host is compared against the IP address of the destination host and through a process known as "Anding," it is determined whether the destination IP address is local or remote.

One of the decisions you will be faced with when implementing TCP/IP on a network is whether you want to use a private IP address range or public IP addresses. Of course, there are disadvantages and advantages to both of them. In making your decisions, keep in mind that any computers having a direct connection to the Internet will obviously require at least one public IP address. But for those computers with no direct Internet connection, you have the option of using public or private addresses.

Three ranges of IP addresses have been reserved, meaning they are not valid on the Internet. So you can use one of these private ranges on your private network. Of course, one of the disadvantages to this is that a proxy server or NAT server is needed for Internet access because the private IP address must be mapped to a public one. In terms of advantages, private IP addressing is more cost effective, can accommodate growth on your network, and can increase security.

If you do decide to implement a **private** IP address range, you can use IP addresses from any of the following classes:

- Class A: 10.0.0.0 – 10.255.255.255
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.16.8.0.0 – 192.168.255.255

There are three different ways that a system can obtain IP configuration information: the computer is assigned a static IP address; the computer is configured to obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server; or the system is configured to locate a DHCP server, but doesn't find one, in which case the system will be assigned a number in the 169.254.0.0 range with a 255.255.0.0 subnet. This is referred to as Automatic Private IP Addressing (APIPA).

Configure and troubleshoot manual TCP/IP configuration

To configure a static IP address on a computer running Windows XP:

1. Right-click My Network Places and click Properties.
2. From the Network Connections window, right-click the appropriate local area connection and click Properties.
3. Select Internet Protocol (TCP/IP) and click the Properties button.
4. Select the option to Use The Following IP Address.
5. Type in a unique IP address, subnet mask, the IP address of the default gateway, as well as the IP address of the primary and secondary DNS server.
6. Click OK.

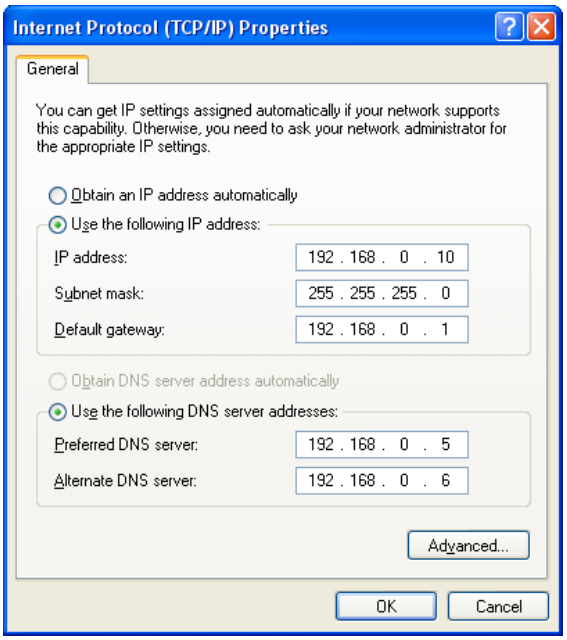

Figure: Configuring TCP/IP in Windows XP

Configure and troubleshoot automated TCP/IP address configuration

A computer running Windows XP can be configured to obtain an IP address from a DHCP server. This means an administrator does not have to manually configure each computer with an IP address. Instead, a server running DHCP is configured with a range of IP addresses that it automatically leases to the computers.

Enabling Automatic Private IP Addressing means the computer will assign itself an IP address in the range of 169.254.0.1–169.254.255.254 if the primary method fails (with the primary method usually being DHCP). This is enabled by default, but you can disable APIPA through the registry. One of the limitations associated with APIPA is that the computer is not assigned any optional parameters such as the IP address of the default gateway or DNS servers. This limits communication to the local subnet with other computers using this method of IP address assignment.

When a computer running Windows XP is configured to obtain an IP address from a DHCP server, another tab is available from the Internet Protocol (TCP/IP) Properties dialog box. This is the Alternate Configuration tab.

This feature is useful if a computer is moved between networks, or if you want a computer to use a specific IP address in the event that a DHCP server is unavailable. For example, if a computer is moved to a network that does not have a DHCP server, the static IP settings configured on the Alternate Configuration tab are used instead. You can enable the Alternate Configuration feature of Windows XP using the following steps:

1. Open the Network Connections applet within the Control Panel.
2. Right-click your Local Area Connection and select Properties.
3. From the list of network components, select Internet Protocol (TCP/IP) and click the Properties button.
4. From the Internet Protocol (TCP/IP) Properties window, select the Alternate Configuration tab.
5. Select the User Configured option, and specify the IP parameters that should be used should the primary IP configuration fail.

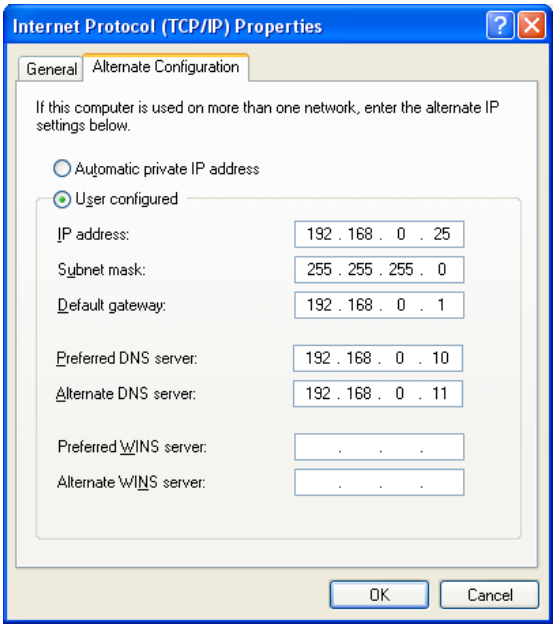

Figure: Windows XP Alternate Configuration

When it comes to troubleshooting IP addressing, you need to know the different utilities that are available. Know that the Ipconfig command can be used to view IP configuration information. There are a number of different parameters that can be used with the command as listed below.

/all	Displays detailed IP configuration information
/release	Releases the IP address for the specified adapter
/renew	Renews the IP address for the specified adapter
/flushDNS	Purges the entries in the DNS cache
/registerDNS	Refreshes all leased IP addresses and re-registers DNS names
/displayDNS	Displays the contents of the DNS cache

Another utility that is useful in troubleshooting IP addressing problems is Ping. You need to know the process that you go through with the ping command to diagnose IP communication problems.

1. Ping the loopback address of 127.0.0.1 to ensure TCP/IP is initialized on the local computer.
2. If successful, ping the IP address assigned to the local computer.
3. Next, ping the IP address of the default gateway. If this fails, verify that the IP address of the default gateway is correct and that the gateway is operational.
4. Next, ping the IP address of a host on a remote network. If this is unsuccessful, verify that the remote host is operational, verify the IP address of the remote host, and verify that all routers and gateways between the local computer and remote computer are operational.

Configure and troubleshoot Internet Connection Firewall settings such as enable and disable

One of the ways that you can protect your computer against Internet attacks is to implement a firewall solution between the Internet and your computer and private network. This is becoming more and more important as people store personal information on their computers such as bank account numbers, credit card data, tax information, and so on. Not implementing a firewall makes this information more accessible to attackers.

By implementing a firewall, you can close the door to your local computer and private network so intruders have a much harder time getting in, but you can still get out. If you are looking for a fast, easy firewall solution, you can take advantage of the firewall component included with Windows XP. This software-based firewall component is known as the **Internet Connection Firewall** (ICF). It allows you to secure your local computer and network by preventing unsolicited traffic from the Internet.

A firewall solution can be a challenge to implement, especially for a user with limited experience. ICF provides a simple method of protecting your computer and requires little to no configuration. You can use it to secure and protect a computer with an Internet connection or, if you are using Internet Connection Sharing (ICS), to protect a small network of computers.

ICF inspects each packet that is destined for the private network. It maintains a table to determine which incoming traffic was initiated on the local network, for example, a user on the private network accessing a Web server on the Internet. Any incoming traffic resulting from this request would be allowed through the firewall. If an inbound request was not initiated by the local computer or a computer on the private network, it is not allowed through the firewall.

ICF will use the following methods to determine which packets to allow through the firewall and which packets to drop:

- Any incoming packets that match a request that was initiated on the private network are allowed through the firewall.
- Any incoming packets explicitly allowed through the firewall by administrator configuration are allowed.
- Any incoming packets that do not match a request that was initiated on the private network are not allowed to pass through the firewall.
- Those incoming packets that will create a new entry in the table are allowed through the firewall.

There may be cases where you need to make resources on your computer available to users on the Internet. In other words, a certain type of traffic initiated on the Internet is allowed to pass through the firewall. This can be done by creating static rules that allow traffic on a specific port to pass through the firewall. For example, if you have a Web server on the private network, you can open up TCP port 80.

Keep in mind that ICF can be used to filter incoming traffic. If you want to filter outgoing traffic, you will need to implement a more sophisticated firewall solution.

Service pack 2 for Windows XP introduced a major change in the Windows Firewall. It is now enabled by default. However, if the default settings have been altered, the Windows Firewall component of Windows XP can be enabled in a number of different ways. For example, you can enable it using the Network Setup Wizard. The Windows Firewall can also be enabled manually using the Network Connection applet in the Control Panel or through the Security Center.

You can use the following steps to enable Windows Firewall:

1. Click Start and click Control Panel.
2. Within the Control Panel, double-click the Network Connections applet. This opens the Network Connections folder.
3. Select the Internet connection you want to protect and click Change Windows Firewall Settings under the list of Network Tasks. An alternate method is to right-click the Internet connection and click Properties.
4. Within the Windows Firewall dialog box, verify that the General tab is active.
5. Click the On (recommended) option. You may also opt to select the Don't allow exceptions option. Click OK.

Once Windows Firewall is enabled, you can select the Exceptions tab to control the flow of data.

Troubleshoot name resolution issues

Configure and troubleshoot Hosts files and DNS

There are two ways that a DNS client can resolve hostnames to IP addresses. A static text file can be used, called a Hosts file, or a DNS server can be used. A Hosts file must contain all the hostname to IP address mappings and it must be manually updated by an administrator. Alternatively, if a DNS server is used, Windows XP clients must be configured with the IP address of the primary DNS server. Clients can then query the DNS server to resolve hostnames.

- If a client is unable to resole a hostname, verify that the Hosts file is properly configured or that the client is configured with the correct IP address for the DNS server.
- Verify that a DNS server is online.
- Nslookup command can be used to send queries to a DNS server.
- IPCONFIG
    - IPCONFIG /DISPLAYDNS - Displays the contents of the DNS cache
    - IPCONFIG /REGISTERDNS - Refreshes leased IP addresses and registered DNS names
    - IPCONFIG /FLUSHDNS - Empties the contents of the DNS cache

Configure and troubleshoot NetBIOS name resolution issues on a client computer

NetBIOS name can be used through a local broadcast, Lmhosts file, or using a WINS server.

- Lmhosts file is a static text file that maps NetBIOS names to IP addresses
    - It is stored in the %SYSTEMROOT%\system32\drivers\etc directory
    - Use the #pre directive to have entries preloaded into the NetBIOS name cache
    - Must be manually updated by an administrator
- WINS provides a dynamic database of NetBIOS name to IP address mappings
    - Clients must be configured with the IP address of the WINS server

Configure and troubleshoot remote connections

Configure and troubleshoot a remote dial-up connection

A new dial-up connection can be created using the Make New Connection wizard. The two connection protocols supported by Windows XP are **Point-to-Point Protocol** (PPP) and **Serial Line Internet Protocol** (SLIP).

- SLIP
    - Supports TCP/IP
    - Used to establish a dial-up connection with a legacy UNIX server
- PPP
    - Supports TCP/IP, NWLink, and NetBEUI
    - Supports DHCP for IP addressing

A user can enable multilink so multiple phone lines can be aggregated. However, in order to do so, the feature must also be enabled on the remote access server.

Remote access authentication protocols include:

- PAP
- SHIVA
- CHAP
- MS-CHAP version 1 and version 2
- EAP

When troubleshooting remote access connections:

- Verify that the modem installed is working and correctly configured (refer to the section "Troubleshooting Hardware Problems" earlier in the chapter).
- Verify the number the user is dialing. Also consider that the problem may exist with the phone line.
- Verify the credentials the user is providing.
- If the user is dialing into a remote access server on your network, check that the remote access service is enabled and started on the server.
- On the server side, verify the availability of ports. If necessary, disconnect any idle sessions or increase the number of available ports.
- If you are using remote access policies to control remote access connections, verify that the remote access policy is not prohibiting the connection.

Configure and troubleshoot a remote connection across the Internet

Virtual private network (VPN) establishes a secure connection across a public network such as the Internet. A tunneling protocol is required to establish a VPN. Windows XP supports two tunneling protocols: **Point-to-Point Tunneling Protocol** (PTP) and **Layer Two Tunneling Protocol** (L2TP).

You can set up a VPN connection in Windows XP by using the steps outlined below:

1. Verify that you have a connection to the Internet.
2. Open the Network Connections applet.
3. From the Network Tasks list, click Create a new connection. Click Next.
4. Select Connection to the network at my workplace. Click Next.
5. Click Virtual Private Network connection. Click Next.
6. Select whether you are using a dial-up or dedicated Internet connection. Click Next.
7. Type in a description for the connection. Click Next.
8. Type in the Host name or IP address of the VPN server. Click Next.
9. If prompted, specify whether or not to use a smart card. Click Next.
10. Click Finish.

Configure and troubleshoot Internet Explorer

Configure and troubleshoot Internet Explorer connections properties

Internet Explorer connection properties are used to configure how the Web browser will connect to the Internet.

The Connections tab available from the Internet Options dialog box will list any Internet connections currently configured on the computer, including dial-up and **Virtual Private Network** (VPN) connections. If a connection to the Internet is through a proxy server, you can use the Settings button to configure the required proxy settings. These settings are summarized in the table below.

Setting	Description
Automatically Detect Settings	Proxy settings and configuration settings are automatically detected.
Use Automatic Configuration Script	Settings are retrieved from a file created by the network administrator. You must also specify the URL to the file or file name.
Use A Proxy Server For This Connection	Specifies that Internet Explorer must connect to the Internet through a proxy server. Provides the address and port number of the proxy server. By selecting the Advance button, you can configure which proxy server and port number to use for different protocols, such as HTTP and FTP. You can then create an exception list. When accessing computers on the exception list, the proxy server is not used.
Bypass Proxy For Local Addresses	Select this option if you do not want to use a proxy server for local (intranet) addresses. Selecting this option can improve performance when accessing computers on your intranet.
Username	For dial-up connections, this is the account name that has been assigned to you by your Internet Service Provider.
Password	The password that has been assigned to you by your Internet Service Provider.
Domain	The domain name assigned to you by your Internet Service Provider.

The connection settings also allow you to configure what Internet Explorer should do when a connection to the Internet is needed. These settings include:

- **Never Dial A Connection -** Internet Explorer will not automatically establish a connection when one is not present but required. A connection must be established manually.
- **Dial Whenever A Network Connection Is Not Present -** Internet Explorer will attempt to establish a connection using your default dial-up connections when a network connection is not available.
- **Always Dial My Default Connection -** Internet Explorer will always attempt to connect using your default dial-up networking connection.

Configure and troubleshoot Internet Explorer security properties

For security purposes, Internet Explorer allows you to place Web sites into different zones. Specific actions can then be performed on Web sites based on the zone it has been placed in. The Security tab available from the Internet Options dialog box displays four separate zones.

Zone	Description
Internet	These contain the majority of other sites that have not been placed in another zone.
Local Intranet	These are the sites that exist within your organization's intranet.
Trusted Sites	These are sites that you trust not to damage your computer and/or data.
Restricted Sites	These sites are considered potentially harmful to your computer and/or data.

A web site can be added to a zone by selecting the specific zone, clicking the Sites button, and typing in the address of the web site.

From the Security tab, you can also set the security level for a zone. For example, sites on an Intranet are more than likely safe, so you can configure a low level of security for the Local Intranet zone. Each zone is configured with a default security level. You can accept the default settings or you can customize the security level to meet your specific needs. The security level for a zone can be changed by moving the slider to low, medium-low, medium, or high. Alternatively, more experienced users can define a custom level of security.

As a Desktop Support Technician, you should keep in mind that the security levels could prevent some loss of functionality when accessing web sites. If a user is trying to access a web site that requires some functionality that is disabled by the security level configured for the zone, add the web site to the list of Trusted Sites.

Configure and troubleshoot Internet Explorer general properties

The following settings can be configured from the General tab of the Internet Options dialog box.

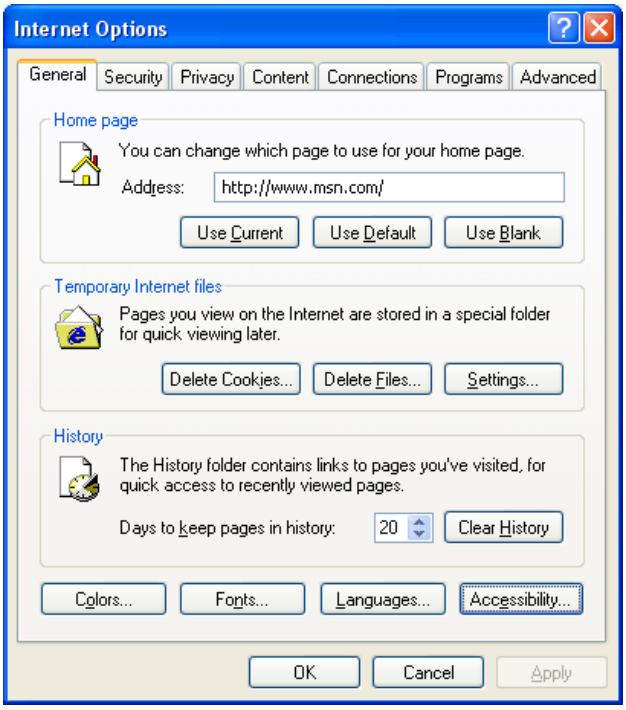

Figure: Internet Options dialog box

- Home Page
  - The home page is the default Web page displayed when Internet Explorer is first opened.
  - By selecting the Use Default button, the home page will be set to that which was configured when Internet Explorer was first installed.
  - The Use Blank button means the home page displayed will be a blank HTML page.
- Temporary Internet files
  - In order to improve performance and reduce the amount of time spent waiting to view web pages, Internet Explorer stores many of the web pages and graphics you have viewed in a folder on your hard drive.
  - Internet Explorer can use the content stored in the Temporary Internet Files folder to display the site content, instead of retrieving them from the web.
  - By selecting the Delete Cookies or the Delete Files button, content in the folder can be deleted.
  - Use the Settings button to configure when stored pages are updated and to configure the amount of disk space allocated to the folder.

- History
  - Internet Explorer will keep links to web page that you have recently viewed and store them in the History folder.
  - By default, links are kept in the History folder for 20 days. If you have a limited amount of disk space, consider lowering this number.
- Colors
  - Configure the color used to display text in Internet Explorer and the color links are displayed in.
- Fonts
  - Configure the fonts to use when a Web page is displayed.
- Languages
  - Configure the language to use when displaying Web pages.
- Accessibility
  - Configure various accessibility options.

Service Pack 2 Internet Explorer Updates

Windows XP service pack 2 includes several new features and enhancements to Internet Explorer. One extremely useful new feature for Internet Explorer is the Manage Add-ons found on the Programs tab. It allows for a finer granularity of control over which add-ons are loaded by Internet Explorer. One of the reasons why it is included in SP2 is because third party add-ons account for a lot of crashes that occur within Internet Explorer. The utility does list all the third party add-ons installed in Internet Explorer and it allows you to disable them individually.

Once you install SP2 for windows XP, you get the functionality of a pop-up blocker without having to download any third party software. The Pop-up Blocker is automatically enabled in Internet Explorer, so most pop-ups should be blocked on your computer.

You can change the settings of the Pop-up Blocker within Internet Explorer by clicking Tools, pointing to Pop-Up Blocker, and selecting Pop-up Blocker Settings. From the dialog box that appears, you can configure IE to allow pop-ups from the Web sites that you specify. You can do this by typing in the URL of the Web site and clicking Add.

Under the Notification and Filter Level, you can configure Internet Explorer to play a sound and show the Information bar when a pop-up is blocked. You can also use the drop-down arrow to change the Filter Level.

Configure and troubleshoot end-user systems by using remote connectivity tools

Use Remote Desktop to configure and troubleshoot an end user's desktop

Remote desktop allows you to take control of one computer from another computer. Before you can do this though, you must enable the Remote Desktop feature. If you are a member of the Administrators group or logged on as the administrator, you can use the following steps:

1. Click Start and select the Control Panel.
2. Double click the System applet.
3. From the System properties dialog box, click the Remote tab.
4. Place a check beside the option to Allow Users To Connect Remotely To This Computer.
5. Click OK to acknowledge Remote Sessions message.
6. Click OK to close the System Properties dialog box.

In order to remotely control a Windows XP computer from a computer running an earlier version of Windows, you must install the Remote Desktop Connection client software. This software must be installed if you are running any of the following operating systems: Windows 95, Windows 98, Windows 98SE, Windows ME, Windows NT 4.0 or Windows 2000. You can find the Remote Desktop Connection client software on the Windows XP CD (either Windows XP Professional or Home edition). If you are running Windows XP, you do not need to install this software because it is installed by default. In any case, you can install the software by inserting your Windows XP CD. From the Welcome page, click Perform Additional tasks. Select the option to Setup Remote Desktop Connection.

Use Remote Assistance to configure and troubleshoot an end user's desktop

Administrators are always looking for more efficient ways to troubleshoot problems as they arise, especially if there are a large number of end users on the network or if there are branch offices that do not have local administrators. Remote Assistance is a tool included with Windows XP that enables administrators and other support persons to remotely assist users with computer problems. Using remote assistance, the expert or assistant can remotely view a user's desktop and take control of a desktop if permission has been granted.

When a user is experiencing technical problems, they can send an invitation for remote assistance to an administrator or other support personnel. An invitation for remote assistance can be sent using Windows Messenger and via an email message. Depending on how remote assistance is configured, an administrator can also offer help to a user without being first explicitly invited. The remote assistance process occurs in three steps:

A user sends a remote access invitation using Windows Messenger or using an email message. The invitation is accepted and a window appears on the assistant's computer displaying the user's desktop. The assistant can view the user's desktop. Interaction with the desktop can only occur if the user enables the Allow Expert Interaction option.

Remote Assistance in Windows XP can be enabled using the System applet within the Control Panel by following these steps:

1. Click Start, and select Control Panel.
2. Within the Control Panel, locate and double-click the System applet.
3. From the System Properties dialog box, select the Remote tab.

4. Under Remote Assistance, enable or disable the option to Allow Remote Assistance Invitations To Be Sent From This Computer.
5. If remote assistance is enabled on the computer, select the Advance button to specify if assistants are permitted to remotely control the local computer. You can also specify how long remote assistance invitations remain open.

Practice Questions

Chapter 1 Installing a Windows Desktop Operating System

1. You are a desktop support technician for your company. Client computers are running Windows XP Professional.

   A new service pack has just been released for Windows XP. You want to deploy the service pack to client computers. What should you do first?

   Select the best answer.

   - ❍ A. Review the documentation for the service pack.
   - ❍ B. Place the installation files for the service pack in a shared network folder.
   - ❍ C. Install the service pack in a test environment.
   - ❍ D. Disconnect all the computers from the network.

2. You are a desktop support technician for a company that supports several users that work from home offices in remote locations.

   One of the users that work from home calls to report that they are unable to install Windows XP. The Information Technology department instructed the user to insert the Windows XP CD and restart the computer. However, setup does not start.

   You determine that the user is attempting to perform an unattended installation, and the winnt sif is located on the floppy disk.

   The user receives a "non-system disk or disk error" message. What should the user do?

   Select the best answer.

   - ❍ A. Change the BIOS settings so the CD-ROM is the first boot device.
   - ❍ B. Copy the winnt.sif to a CD.
   - ❍ C. Rename the winnt.sif to unattend.txt.
   - ❍ D. Remove the floppy disk from the floppy drive and restart the computer.

3. You are the desktop support technician for your company. You are assisting in the deployment of Microsoft Windows XP Professional on a new workstation.

   You are using Remote Installation Services (RIS) to deploy the operating system. When you boot the computer, you receive the following error message:

   Operating system not found

   You verify that the workstation is using a PXE-compliant network adapter. You want the workstation to automatically connect to the RIS server. What should you do?

   Select the best answer.

   - ❍ A. Configure the computer's BIOS to boot from the CD-ROM.
   - ❍ B. Verify that an IP address has been reserved for the new computer on the DHCP server.
   - ❍ C. Create a Remote Installation Services boot disk.
   - ❍ D. Change the computer's BIOS settings to boot from the PXE network adapter.

4. You are a help desk technician for your company. You have installed Windows XP Professional on a computer with a single hard drive. The C drive has been formatted with NTFS.

   You decide to dual-boot Windows XP Professional with Windows 98. You need to convert the C drive back to FAT32. What should you do?

   Select the best answer.

   - ❍ A. Reformat the partition and restore the data from backup.
   - ❍ B. Run convert C:/FS:FAT.
   - ❍ C. Run convert C:/FS:NTFS.
   - ❍ D. Use System Restore to recover the previous disk configuration.

5. You are a desktop support technician for your company. All workstations are currently running Microsoft Windows 2000 Professional.

   A new computer has been purchased for one of the managers. The new computer is running Microsoft Windows XP Professional. You want to move the user's files, folders, and settings to the new computer. What should you do?

   Select the best answer.

   - ❍ A. Use the Files and Settings transfer wizard.
   - ❍ B. Copy the NTUSER.DAT file to the Windows XP computer.
   - ❍ C. Use the System Restore utility.
   - ❍ D. Connect the two computers to the network. Manually copy the files and folders to the new computer.

6. You are the desktop support technician for your company. A user has installed Microsoft Windows XP Professional and Microsoft Windows 98 on their computer.

   Windows XP Professional is installed on partition C. Windows 98 has been installed on partition D. The user reports that he is unable to run Microsoft Office 2000 under Windows 98. The problem does not occur when he is running Windows XP Professional. How should the user resolve the problem?

   Select the best answer.

   - ❍ A. Boot into Windows XP Professional and edit the permissions for the application executables.
   - ❍ B. Install Microsoft Office 2000 under Windows 98.
   - ❍ C. Create a third partition. Reinstall Microsoft Office 2000 on the new partition.
   - ❍ D. Format the D partition with NTFS.

7. You are a help desk support technician for your company. You need to dual-boot Computer01 with Windows XP Professional. The computer is currently running Windows NT Workstation 4.0 with service pack 3. Which file system should you use for the active partition?

   Select the best answer.

   - ❍ A. FAT
   - ❍ B. EFS
   - ❍ C. NTFS
   - ❍ D. FAT32

8. You are a desktop support technician for your company. A member of the Developers department requires a computer running both Microsoft Windows 2000 Professional and Microsoft Windows XP Professional. What should you do?
Select the two best answers.

- ❑ A. Install Windows XP, and then Windows 2000.
- ❑ B. Use a unique computer name for each installation.
- ❑ C. Install Windows 2000, and then Windows XP.
- ❑ D. Use the same computer name for each installation.

Chapter 2 Managing and Troubleshoooting Access to Resources

1. John is a member of the Engineers group and the Managers group. He is also a director within the company, which gives him special privileges to specific accounting information regarding his division. John needs to have the ability to read, modify, and create new files within the directory C:\MARKETING. You check the permissions for that directory and find that members of the Managers group have Read and Write permissions. Engineers have Deny all permissions, and as a director, he's been directly assigned Full Control over that directory. What is John able to do with the data in this directory?

   Select the best answer.

   - ❍ A. He can view it, but not change it.
   - ❍ B. He can modify it, but not add new files.
   - ❍ C. He can do nothing.
   - ❍ D. He can add new files, but not change anything once it has been saved.

2. You are a desktop support technician for your company. All workstations are running Microsoft Windows XP Professional.

   A user on the network uses his mobile computer in the office and at home. He has access to a file stored in a network share when he is out of the office and working offline. He does not have to manually copy the folder to his hard drive.

   The user calls to report that he is no longer able to open the file when he is working offline. You need to ensure that the user has access to the file all the time. What should you do?

   Select the best answer.

   - ❍ A. Enable offline files check box on the Offline Files tab from the Folder Options window.
   - ❍ B. Increase the amount of hard disk space allocated to offline files.
   - ❍ C. Verify that the Allowed caching of files in this shared folder check box is selected for the network share.
   - ❍ D. Right-click the file in the network share and select Make Available Offline from the context menu.

3. You are the desktop support technician for your company. All workstations are running Microsoft Windows XP Professional.
A user calls to report that they have attached a printer to their computer. When they attempt to print a document through Microsoft Word, the characters are garbled on the page.
You determine that the problem occurs when printing from any application. The problem continues to occur after restarting the printer. What should you do?
Select the best answer.

- ❍ A. Reinstall the printer driver.
- ❍ B. Empty the contents of the print queue.
- ❍ C. Repair the installation of Microsoft Word.
- ❍ D. Install the print device on another computer.

4. You are the desktop support technician for your company. All workstations are running Microsoft Windows XP Professional.

A user has the NTFS Modify permission and the Read share permission in a folder called Sales When he accesses the files in the Sales folder locally, he can save his changes. However, when he opens the files in the Sales folder from across the network, he is unable to modify them. What is causing the problem?

Select the two best answers.

- ❍ A. The user's effective permission is Read.
- ❍ B. The user's effective permission is Deny.
- ❍ C. Share permissions are not evaluated when accessing the folder locally.
- ❍ D. NTFS permissions only apply locally.

Chapter 3 Configuring and Troubleshooting Hardware Devices and Drivers

1. You are the desktop support technician for your company. All computers are running Windows XP Professional.

ICS is enabled on Computer A. The Internet connection is shared between 8 computers. A user reports that they are unable to access the Internet. You soon discover that the problem is affecting all computers on the network. What should you do first to verify that the modem on Computer A is functioning correctly?

Select the best answer.

- ❍ A. Use Network Monitor to monitor traffic to and from the computer.
- ❍ B. Use System Monitor to monitor network counters.
- ❍ C. Use Device Manager to check the device status.
- ❍ D. Enable modem logging using the Modem applet within the Control Panel.

2. You are the desktop support technician for your company. You are installing Windows XP Professional on a mobile computer for a user.

   The mobile computer is configured with a modem and an Ethernet PC card. The mobile computer is connected to a docking station in the office and uses the Ethernet card to connect to the network. At home, the user connects to the company network using dial-up networking. You want to disable the network card when the user is working from home. There is currently a single hardware profile configured called Docked. What should you do?

   Select the best answer.

   - ❍ A. Modify the Device Manager settings to disable all devices used by the docked hardware profile.
   - ❍ B. Create another hardware profile called Undocked. In control panel, disable the server service in the services options.
   - ❍ C. Create a second hardware profile. In the Control Panel, place this profile at the top of the list.
   - ❍ D. Create a new hardware profile named Remote. Use Device Manager to disable the Ethernet PC card devices for this hardware profile.

3. You are the desktop support technician for Adventure Works. All workstations and mobile computers are running Microsoft Windows XP Professional.

   A user calls for assistance with configuring the power settings on his mobile computer. The user does not want his monitor to shut down while his computer is idle. He indicates that he always has his mobile computer plugged into a power outlet.

   You need to recommend a power scheme. Which power scheme should you recommend?

   Select the best answer.

   - ❍ A. Always On
   - ❍ B. Portable/Laptop
   - ❍ C. Minimal Power Management
   - ❍ D. Presentation

Chapter 4 Configuring and Troubleshooting the Desktop and User Environments

1. You are a desktop support technician for a small company. The client computers have been upgraded to Microsoft Windows XP Professional.

   Security settings on client computers are configured using a security template. All computers must be configured with identical security settings.

   A user reports that they are prompted to change their password more frequently than normal. You suspect that changes have been made to the security settings. What should you do to determine if the security settings have changed?

   Select the best answer.

   - ❍ A. Use the Security Templates console to compare the existing settings with those in the template.
   - ❍ B. Launch Active Directory Users and Computer. Open the appropriate group policy and analyze the existing settings.
   - ❍ C. Launch the Resultant Set of Policy to view the existing settings configured on the computer.
   - ❍ D. Launch Security Configuration and Analysis. Compare the existing settings against those in the template.

2. You are a desktop support technician for your company. Client computers on the network are running Microsoft Windows XP Professional. All computers are members of an Active Directory domain.

   Changes have recently been made to the network security policies. A local security policy has also been configured on each computer.

   You want to determine the effective security settings on a Windows XP computer. What should you do?

   Select the best answer.

   - ❍ A. Use the Resultant Set of policy in planning mode.
   - ❍ B. Use Security Configuration and Analysis.
   - ❍ C. Use IP Security Monitor.
   - ❍ D. Use Resultant Set of Policy in logging mode.

3. You are a desktop support technician for your company. Microsoft Windows XP Professional is installed on all workstations.

   Workstations are shared between users. Users are members of the local Power Users group on their workstation.

   A specific set of desktop icons and shortcuts must be visible on the desktop for each user that logs onto the workstation. Users must also be able to customize their desktop by adding their own shortcuts and icons in addition to the default ones.

   You want to prevent users from removing the icons and shortcuts on the default desktop. What should you do?

   Select the best answer.

   - ❍ A. Remove the Modify permission on the C:\Documents and Settings\All Users directory for the Power Users group.
   - ❍ B. Remove the Modify permission on the C:\Document and Settings\%username% directory.
   - ❍ C. Deny the Full Control permission on the C:\Documents and Settings directory for the Power Users group.
   - ❍ D. Deny Full Control permission on the C:\Documents and Settings\Default User directory.

4. You are the desktop support technician for your company. A member of the Developers department needs to be able to establish a remote desktop session with a computer running Windows XP Professional. You need to allow the user permission to connect, while implementing the principle of least privilege. What group should you add the user to?

   Select the best answer.

   - ❍ A. Add the user to the Users group.
   - ❍ B. Add the user to the Power Users group.
   - ❍ C. Add the user to the Remote Desktop Users group.
   - ❍ D. Administrators

5. You are a desktop support technician for a large enterprise company. The head office is located in New York and a branch office in Paris.

   One of the managers travels between the two offices. When he returns from a business trip to the branch office, his laptop computer is displaying the date and time in French. His email messages are now displaying the date and time in French.

   You need to change the date and time settings back to English. What should you do?

   Select the best answer.

   - ❍ A. Apply the English (United States) Standards and Formats in the Regional and Language options.
   - ❍ B. Change the Time Zone to Eastern Time (US&Canada) in the Date and Time Options.
   - ❍ C. Apply the English input language keyboard in the Regional and Language Options.
   - ❍ D. Select the English language in the Date and Time options.

Chapter 5 Troubleshooting Network Protocols and Services

1. You are a desktop support technician for your company. Client computers are running Microsof Windows XP Professional.

   The network administrator has recently made changes to the zone database file on the DNS server. A user reports that they are having problems resolving hostnames.
   You suspect the client resolver cache may have outdated entries. What should you do?

   Select the best answer.

   - ❍ A. Execute the ipconfig command with the /all parameter.
   - ❍ B. Execute the ipconfig command with the /flushdns parameter.
   - ❍ C. Execute the ipconfig command with the /displaydns parameter.
   - ❍ D. Execute the ipconfig command with the /renew parameter.

2. You are a desktop support technician for your company. All client computers are running Microsoft Windows XP Professional.

   A client has reported that his laptop cannot see other computers on the network. You execute the IPCONFIG /All command on the laptop and find that the current IP address is 169.254.255.13. You are unable to PING the DHCP server from the user's laptop. What is the problem and the solution?

   Select the best answer.

   - ❍ A. The IP address lease has expired on the laptop. You should execute the command IPCONFIG /RELEASE.
   - ❍ B. The IP address lease has expired on the laptop. You should execute the IPCONFIG /RELEASE and IPCONFIG /RENEW commands.
   - ❍ C. The laptop cannot communicate with the DHCP server. The user should assign a static IP address and subnet mask to gain access to the network.
   - ❍ D. The laptop cannot communicate with the DHCP server. At a command prompt window on the laptop, you should execute the IPCONFIG /RELEASE and IPCONFIG /RENEW commands to release the current IP address and request a new lease from the DHCP server.

3. You are the desktop support technician for an Internet Service Provider. A user reports that they have enabled ICS on one computer. The Internet connection is shared between 8 computers. All computers are running Windows XP Professional.

   The Internet is not accessible from one of the user's computers. However, this problem is not affecting any other computers on the network. What should you instruct the user to do?

   Select the best answer.

   - ❍ A. Open the Event Viewer. Check the System log for any errors.
   - ❍ B. Use the IPCONFIG command on the ICS computer. Verify the IP address assigned to the LAN connection.
   - ❍ C. Issue the PING command on the ICS computer to verify Internet connectivity.
   - ❍ D. Use the IPCONFIG command. Verify the IP parameters configured on the computer.

4. You are the desktop support technician for your company. All workstations are running Microsoft Windows XP Professional.

   A user calls to report that Internet Explorer is sluggish when loading Web pages that she has previously visited.

   You need to improve performance. What should you do?

   Select the best answer.

   - ❍ A. Decrease the number of days that Internet Explorer will keep track of pages in your History folder.
   - ❍ B. Decrease the maximum size of the Temporary Internet Files folder.
   - ❍ C. Delete the contents of the Temporary Internet Files folder.
   - ❍ D. Increase the amount of disk space allocated to the Temporary Internet Files folder.

5. You are the desktop support technician for your company. All computers have been upgraded to Microsoft Windows XP Professional.

   Users report that they are receiving errors when trying to resolve certain hostnames. You need to determine if the problem is DNS related. Which command can you use?

   Select the best answer.

   - ❍ A. nslookup
   - ❍ B. ipconfig
   - ❍ C. Tracert
   - ❍ D. Ipconfig /registerdns

Answers and Explanations

Chapter 1

1. Answer: A

Explanation A. Before you attempt to install the service pack, or any other software, you should review the documentation.

Explanation B. A service pack can be installed from a network location. However, before deploying the software, you should read the documentation.

Explanation C. The installation of service packs can have adverse effects; they should be installed and tested within a test environment before being deployed on production computers. However, in many cases, this is not an option.

Explanation D. It is not necessary to disconnect computers from the network when installing a service pack.

2. Answer: A

Explanation A. The computer must be configured to boot from the CD-ROM device. The computer is configured to boot from the floppy drive, which is why the error message is appearing.

Explanation B. The winnt.sif is used to perform an unattended installation. This file must be named winnt.sif and it must be placed on a floppy disk, not a CD.

Explanation C. The winnt.sif is used to perform an unattended installation. This file must be named winnt.sif and it must be placed on a floppy disk, not a CD.

Explanation D. You should not remove the floppy diskette. Setup will look for this file during the installation of Windows XP. Once the boot order is changed in the BIOS, the error message will no longer appear.

3. Answer: D

Explanation A. The computer does not need to be configured to boot from the CD-ROM. This is required if you are installing Windows XP locally from a Windows XP CD.

Explanation B. The computer does not require a reserved IP address. The computer is assigned a dynamic IP address from the DHCP server.

Explanation C. A Remote Installation Services boot disk is only required if the computer is not configured with a PXE network adapter. The scenario indicates that the computer has a PXE network adapter installed.

Explanation D. The BIOS on the computer must be configured to boot from the PXE network adapter. Otherwise, you will receive an operating system not found error message.

4. Answer: A

Explanation A. You should reformat the partition and restore the data from backup. To change from NTFS to FAT32, a partition must be formatted.

Explanation B. The convert command can be used to change from FAT32 to NTFS, not vice versa.

Explanation C. This command is used to convert a partition from FAT32 to NTFS.

Explanation D. The System Restore cannot be used to recover from a file system change.

5. Answer: A

Explanation A. The Files and Settings Transfer wizard included with Windows XP is used to move files, folders, and settings from an old computer to a new computer.

Explanation B. You should not copy the NTUSER.DAT to the new computer. This file contains profile settings. Copying it between the two computers will not transfer the users files, folders, and settings.

Explanation C. You cannot use the System Restore utility. This is used to restore a computer running Windows XP to a previous state.

Explanation D. Although this is one way of transferring the files and folders to the new computer, it does not copy over the user's settings.

6. Answer: B

Explanation A. Permissions for the executables have not been changed, so the user has permission to run all the applications.

Explanation B. To run the applications under both operating systems, the user must install Microsoft Office 2000 twice.

Explanation C. Installing Microsoft Office 2000 on a different partition will not resolve the issue. The application must be installed under each operating system.

Explanation D. Changing the file system will not resolve the issue. Also, Windows 98 does not support NTFS, which means anything stored on this partition would be inaccessible.

7. Answer: A

Explanation A. You must use FAT on the active partition. Windows NT Workstation 4.0 does not support the version of NTFS included with Windows XP unless service pack 4 is installed. Therefore, you must use FAT.

Explanation B. The Encrypting File System (EFS) is used for encrypting folders.

Explanation C. Windows NT Workstation 4.0 does not include the version of NTFS included with Windows XP unless the latest service pack has been applied.

Explanation D. Windows NT Workstation 4.0 does not support FAT32. Therefore, you cannot use this file system on the active partition.

8. Answers: B, C

Explanation A. When dual-booting, it is generally recommended that you install the most recent version of Windows last.

Explanation B. You must use a unique computer name for each operating system instance.

Explanation C. When dual-booting two versions of Windows, the newest version should be installed last. Therefore, Windows 2000 should be installed first followed by Windows XP.

Explanation D. A unique computer name is required for each instance of the operating system.

Chapter 2

1. Answer: C

Explanation A. John has assigned the Deny All permission as a result of his membership in the Engineers group. Therefore, he cannot view the data in the directory.

Explanation B. John has assigned the Deny All permission as a result of his membership in the Engineers group. Therefore, he cannot modify the data in the directory.

Explanation C. One of John's permissions is Deny All, which overrides all others.

Explanation D. John has assigned the Deny All permission as a result of his membership in the Engineers group. Therefore, he cannot add any new data to the directory.

2. Answer: B

Explanation A. You do not need to enable offline files. This option is already enabled, as indicated by the scenario.

Explanation B. By default, 10% of the available hard disk space is allocated to temporary offline files. The user will not be able to open the file if this amount of space is exceeded. You should increase the amount of hard disk space allocated to offline files.

Explanation C. This option is already configured if the user has successfully cached the file stored in the network share before.

Explanation D. Manually making the file available offline will not resolve the problem. The maximum amount of disk space allocated to offline files on the user's computer has been reached.

3. Answer: A

Explanation A. If the characters appear garbled on the page, you should reinstall or update the printer driver.

Explanation B. Deleting the documents on the print queue will not solve the problem. A problem with the print queue will not result in characters being printed incorrectly.

Explanation C. This will not resolve the problem. You have already discovered that the problem is not specific to one application.

Explanation D. It is not necessary to install the print device on another computer. Although the print device may work correctly on another computer, it is an inefficient solution to the problem.

4. Answers: A, C

Explanation A. When accessing resources across the network, the effective permission is a combination of the share and NTFS permissions. The most restrictive permission is the effective permission.

Explanation B. If the effective permission was Deny, the user would not be able to access the files in the folder.

Explanation C. Share permissions are only applied when accessing resources from across the network.

Explanation D. NTFS permissions are applied when accessing resources locally or across the network. A user's effective permission when accessing a resource from across the network is a combination of share and NTFS permissions, with the most restrictive permission being the effective permission.

Chapter 3

1. Answer: C

Explanation A. Network Monitor is used to capture and analyze network traffic. It is not used to determine if a modem is functioning correctly.

Explanation B. System Monitor is not used to determine whether a modem is functioning. It is used to gather performance statistics.

Explanation C. Device manager can be used to verify that a device is functioning properly.

Explanation D. Windows XP uses the Phone and Modem applet, not the modem applet. Modem logging can be used to troubleshoot a failing dial-up networking connection.

2. Answer: D

Explanation A. You should not disable all the devices used by the docked hardware profile. The only device you may want to disable for the docked hardware profile is the modem.

Explanation B. You should not disable the Server service.

Explanation C. Changing the order that the hardware profiles appear will not resolve the problem. The network card will still be enabled when the user is connecting from home.

Explanation D. Create a second hardware profile named Remote and disable the Ethernet PC card for the new profile. Instruct the user to select this hardware profile when working from home.

3. Answer: D

Explanation A. The Always On power scheme turns off the monitor after 20 minutes if the computer is plugged into a power source.

Explanation B. The Portable/Laptop power scheme will turn off the monitor after 2 hours if the computer is plugged into a power source.

Explanation C. The Minimal Power Management scheme will turn off the monitor whether it is plugged into a power source or running on battery.

Explanation D. The Presentation power scheme will not turn off the monitor as long as the computer is plugged into a power source. If the computer is running off a battery, it will be placed in system standby mode.

Chapter 4

1. Answer: D

Explanation A. The Security Templates console is not used for this purpose. It is used to create and configure security templates.

Explanation B. The Active Directory Users and Computers console is used to administer OUs, computers, and user accounts. The scenario does not indicate whether or not the computers are members of a domain.

Explanation C. Resultant Set of Policy is used to determine the effective settings when multiple policies exist. It cannot be used to compare the settings configured on a computer to those in a template.

Explanation D. Security Configuration and Analysis can be used to compare the security settings configured on a local computer with those in a security template to identify any discrepancies.

2. Answer: D

Explanation A. Resultant Set of Policy in planning mode is used to view the impact any policy changes will have before making the change in the production environment.

Explanation B. This tool is used to view and manage policy settings.

Explanation C. IP Security Monitor is used to monitor IPSec communications between hosts.

Explanation D. RSoP can help you determine the final set of policies that are applied and track down policy precedence, making troubleshooting easier.

3. Answer: A

Explanation A. By default, the Power Users group is assigned the Modify permission to the C:\Documents and Settings\All Users directory. By removing this permission, users will not be able to remove the default icons and shortcuts placed within the directory.

Explanation B. You should not remove the Modify permission on each user's profile directory. This will prevent the users from modifying their desktops.

Explanation C. You should not deny Full Control permission on the C:\Documents and Settings directory. This will prevent all users from even having the permission to read the contents of the folder, thereby making profiles inaccessible.

Explanation D. You should not deny Full Control permission on the C:\Documents and Settings\Default User directory. The Default User directory will be inaccessible to all members of the Power Users group.

4. Answer: C

Explanation A. The Users group is not assigned the permissions required to establish a remote desktop session.

Explanation B. The Power Users group does not have permission to establish a remote desktop session.

Explanation C. By adding the user to this group, he or she will have the permissions required to establish a remote desktop session.

Explanation D. You should not add the user to the Administrators group. While this would grant the user the ability to connect with Remote Desktop, this goes against the principle of least privilege. The user will have more permissions than they require.

5. Answer: A

Explanation A. The Standards and Formats determine how programs format numbers, currencies, date and time. You need to apply the English (United States) Standards and Formats in the Regional and Language options.

Explanation B. This determines the time that is displayed in the system tray.

Explanation C. This determines the language you use to insert text.

Explanation D. This determines the time that is displayed in the system tray.

Chapter 5

1. Answer: B

Explanation A. The "all" parameter displays the client's IP configuration.

Explanation B. The cache on the Windows XP Professional client can be cleared using the ipconfig command with the flushdns parameter.

Explanation C. The "displaydns" parameter displays the contents of the cache.

Explanation D. The renew parameter renews the client's IP address with the DHCP server.

2. Answer: B

Explanation A. The IP address lease has expired, but the IPCONFIG /RELEASE will only release the current IP address. A new IP address must be requested as well.

Explanation B. The IP address lease has expired and assigned the address of 169.254.255.29 because it has not received a new IP address from the DHCP server. At a command prompt window on the laptop, you should execute the IPCONFIG /RELEASE and IPCONFIG /RENEW commands to release the current IP address and request a new lease from the DHCP server.

Explanation C. The laptop is able to communicate with the DHCP server because PING was successful.

Explanation D. The laptop is able to communicate with the DHCP server, because PING was successful.

3. Answer: D

Explanation A. Although this might provide information about the problem, the first logical step would be to verify that the client computer is properly configured.

Explanation B. Since the problem is not affecting any other client computers, the ICS computer is already properly configured.

Explanation C. Since the problem is not affecting any other client computers, the ICS computer must already be properly configured.

Explanation D. The first logical step in troubleshooting the problem is to verify that TCP/IP is properly configured on the client computer.

4. Answer: D

Explanation A. The History folder stores links to previously viewed Web sites. These links are used to quickly access a Web site.

Explanation B. You should not decrease the size of the Temporary Internet Files folder. This will not improve performance, but instead slow performance even more.

Explanation C. You should not delete the contents of the folder. This will decrease performance, as Internet Explorer will have to obtain Web content from the Internet instead of from the local computer.

Explanation D. By increasing the amount of disk space, Internet Explorer can store more information in the Temporary Internet Files folder. There will be an increase in performance at the expense of consuming more disk space.

5. Answer: A

Explanation A. You can use the nslookup command to test name resolution. If you are not successful in using nslookup, the problem is likely DNS related.

Explanation B. This command is not used to test host name resolution. It is used to view and manipulate TCP/IP settings on the local computer.

Explanation C. This command is used to identify the path a packet takes to reach a destination host.

Explanation D. This command registers a computers hostname with a DNS server. However, it does not test hostname resolution.