Exam
Manual

LearnSmart

Microsoft (70-272) Windows XP Troubleshooting Desktop Apps

This LearnSmart exam manual breaks down the most important concepts you need to know in order to pass the Windows XP Desktop Applications exam (70-272). By studying this manual, you will become familiar with an array of exam-related topics, including:

- Configuring and troubleshooting applications
- Resolving issues related to application customization
- Configuring application security
- And more!

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

Troubleshooting Desktop Applications (70-272) LearnSmart Exam Manual

Product ID: 010323
Production Date: July 19, 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@preplogic.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 Desktop Application on a Microsoft Windows XP Operating System (70-272) exam. This exam covers the following topics: email accounts, newsgroups, application security, name resolution, and security permissions.

What to Know

Exam topics include:

- Configure and troubleshoot Office applications
- Troubleshoot application installation errors
- Configure and troubleshoot e-mail account settings
- Configure and troubleshoot Internet Explorer
- Configure and troubleshoot Outlook Express
- Troubleshoot multi-boot computers
- Interpret application error messages
- Configure and troubleshoot devices
- Import and export data in an Office application
- Configure operating system features
- Troubleshoot name resolution
- Troubleshoot remote access
- Configure and troubleshoot TCP/IP
- Implement and troubleshoot ICF
- Identify virus attacks
- Apply critical updates

Take time to review the Exam Objectives from Microsoft at:
http://www.microsoft.com/learning/exams/70-272.asp

Tips

This exam is 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 related to configuring, managing, and troubleshooting desktop applications in 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 application installations, setting up e-mail accounts, configuring Internet Explorer, managing dial-up remote access, IP addressing, and so on.

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. Evaluation versions of virtual computer software are available.

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.

Configuring and Troubleshooting Applications

Configure and troubleshoot Office applications

Set application compatibility settings

Some legacy programs may not function properly after Windows XP has been installed. In such cases, you can run the Program Compatibility Wizard included with Windows XP on the program's Setup file. The file may be called setup.exe (or something similar) and will be located on the program's installation disk. You can launch and run the Program Compatibility Wizard using the steps outlined below:

1. Click Start, All Programs, Accessories, and click Program Compatibility Wizard.
2. Click Next.
3. Select one of the options for locating the program. You can select from the following: I want to choose from a list of programs, I want to use the program in the CD-ROM, or I want to locate the program manually.
4. Click Next.
5. Once you locate the program, select a program compatibility mode. Click Next.
6. Select the display settings for the program. Click Next.
7. Click Next to test the program with the new compatibility settings.

Once the settings have been tested, you have the option of keeping the settings, abandoning them, or trying different settings. There is a good possibility that you may need to run the wizard more than once to you find the right compatibility settings for your program.

More experienced users may choose to set the compatibility settings for a program manually instead of using the Program Compatibility Wizard. You can manually configure compatibility settings using the steps outlined below:

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.

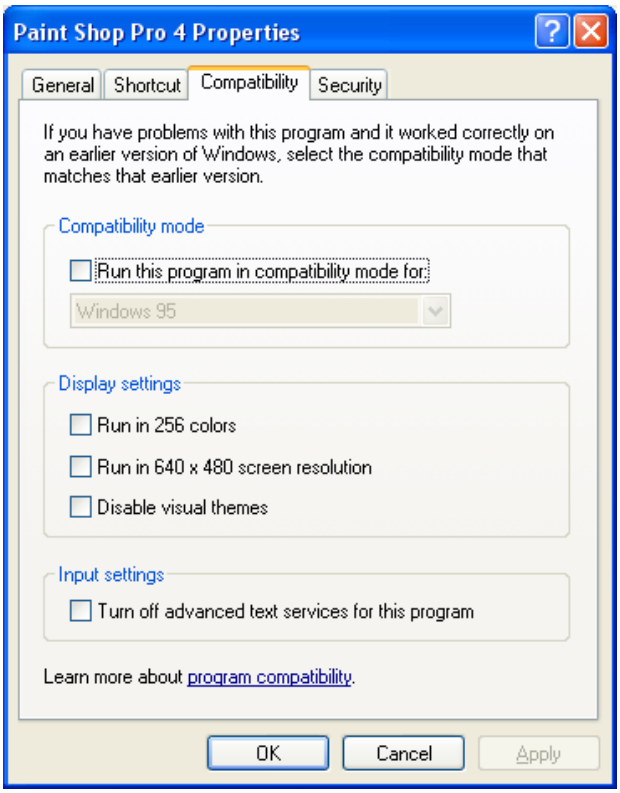

Figure: Compatibility tab used to configure application compatibility settings

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.

Another option available for getting programs to function under Windows XP is to use an application called QFIXAPP (Quick Fix Utility). You can find the application in the Application Compatibility Toolkit for Windows XP and Windows Server 2003. QFIXAPP can be used to apply various program fixes. It will provide you with a list of available program fixes from which you can choose the fixes you want to apply. You can find more information about the application at 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. However, it 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.

Troubleshoot application installation problems

When application installation problems occur, it is the job of the Desktop Support Technician to troubleshoot and resolve them. If problems occur during the actual installation, there are some basic guidelines you can follow to determine the causes:

- If Microsoft Office is being installed from CD, make sure the CD is not damaged.
- Verify that the CD-ROM is functioning correctly.
- If Microsoft Office is being installed across the network, make sure the desktop and the server hosting the installation point have network connectivity.
- Verify that an installation point has been set up for a network installation.

Log files can also be used to troubleshoot problems with a Microsoft Office installation. Setup automatically creates two log files, the Setup log file and the Windows Installer log file, and stores them in the \Temp directory.

Microsoft Office setup includes a maintenance mode. You can rerun setup in this mode at any time to resolve various problems that include:

- Adding features that were not added during the installation of Microsoft Office
- Repairing corrupt program files and registry settings

The Microsoft Office setup program can be run in maintenance mode using the following steps:

1. Within the Control Panel, double-click the Add Or Remove Programs utility.
2. From the list of installed programs, select Microsoft Office XP.
3. Click the Change Or Remove button.
4. From the Setup dialog box, click one of the available options: Add Or Remove Features, Repair Office, Detect And Repair Errors In My Office Installation, or Uninstall Office.

Configure and troubleshoot e-mail account settings

Before you can send and receive e-mail using Microsoft Outlook, you must create at least one e-mail account. You can create a new e-mail account in Outlook using the steps listed below:

1. From the Tools menu, select the E-mail Accounts option.
2. Choose the View Or Change Existing E-mail Accounts option. Click Next.
3. Click Add button and choose the type of mail server for the new account. The options available are Microsoft Exchange Server, POP3, IMAP, HTTP, and Additional Server Types. Click Next.
4. Enter the User Information, Server Information, and Logon Information in the Internet E-Mail Settings dialog box. Click Next.
5. The E-mail Accounts dialog box will display all of the Email accounts configured with Outlook. Click Finish to close the window.
6. Click Finish to complete the Internet Connection Wizard.

The properties of an existing Microsoft Outlook e-mail account can be modified at any time by following the procedure described below:

1. From the Tools menu, select the E-mail Accounts option.
2. Select the View or change existing e-mail accounts option. Click Next.
3. Select the account you want to modify and click the Change button. The same window that you use to create the E-mail account is displayed. The standard settings can be modified from this window.
4. Click the More Settings button to modify additional settings. The Internet E-mail Settings window includes the General, Outgoing Server, Connection and Advanced tabs.
5. Modify the required settings and click OK to apply the changes.
6. Click the Next button to return to the E-mail Accounts window and then click Finish.

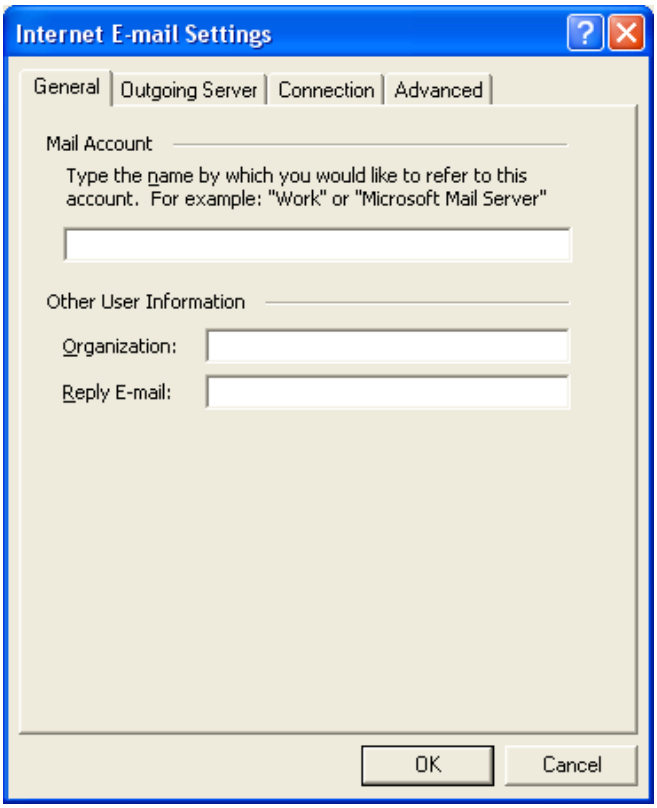

Figure: Modifying e-mail account settings in Outlook

Outlook can be configured with multiple e-mail accounts. For example, you may have a work account and a personal account. The problem is that all e-mail messages are received into the same Inbox. This can make it difficult to manage messages from multiple accounts.

A simple way to organize Outlook if there are multiple e-mail accounts is to set up multiple inboxes. You can then create rules to have messages from a specific e-mail account moved to a specific inbox. You can create multiple inboxes using the steps described below:

1. If the folder list is not visible in Outlook, click the Folder List option from the View menu.
2. Right-click the Inbox folder and select New Folder. The Create New Folder dialog box is opened.
3. Enter the Name of the new folder in the Name text box.
4. Select the type of folder you are creating from the Folder contains drop down list.
5. Select the location where the folder will be located. If you are creating a Mail folder, select the Inbox folder.
6. Click OK. The new folder will appear under the Inbox folder.

Configure and troubleshoot Internet Explorer

Users can configure various settings within Internet Explorer to meet their specific needs. For example, from the View menu, users can configure the Toolbars they want displayed. One new feature that has been introduced in Windows XP service pack 2 is the Pop-up Blocker. The Pop-up Blocker is automatically enabled by 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 for the Web sites that you specify. You can do this by typing in the URL of the Web site and clicking Add.

In the Notification And Filter Level area, 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.

General Settings

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

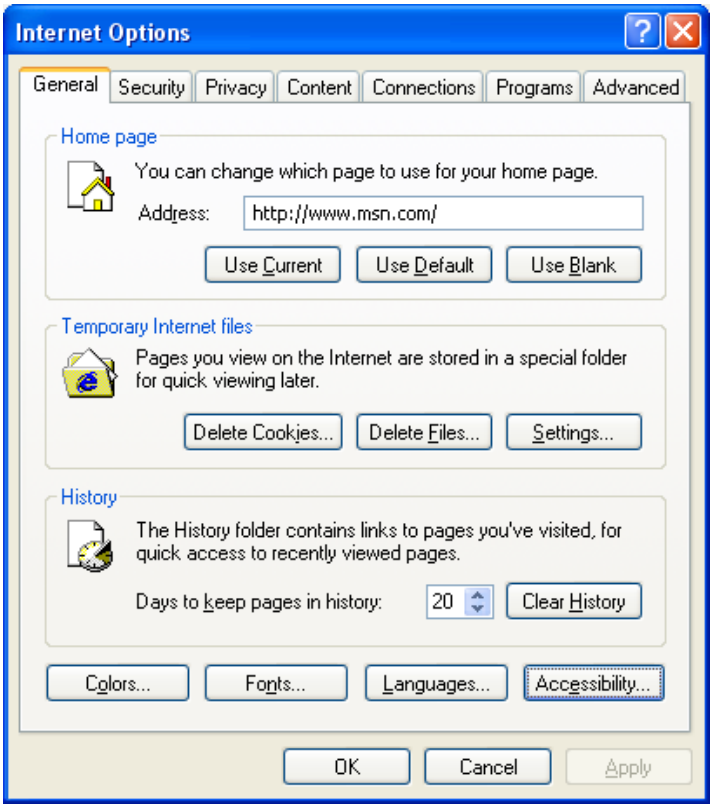

Figure: Internet Options dialog box

- Home Page
  - The home page is the Web page that is always displayed when the browser is first opened or when the Home button is clicked. Businesses often change the home page to a site on their intranet.
  - 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 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. This improves privacy by reducing the risk that someone will be able to determine which Web sites another user has visited.
    - Use the Settings button to configure when stored pages are updated and to configure the amount of disk space allocated to the folder. For best performance, store the temporary Internet files on a different disk than the Windows system files.
- History
    - Internet Explorer will keep track of the Web pages that you have recently visited and store them in the History folder. You can easily return to one of these Web pages by clicking the History button in Internet Explorer and clicking one of the links.
    - By default, links are kept in the History folder for 20 days. You can reduce this value if you have limited disk space.
    - To improve privacy by reducing the risk of other people seeing which Web sites a user has visited, press the Clear History button.
- 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.

When you are configuring the Temporary Internet Files settings, you can configure how and when Internet Explorer should check for updates. Internet Explorer can be configured to take any of the following actions:

- Every Visit To The Page
    - When you return to a Web page you have previously viewed, Internet Explorer will check for updates to the page. Keep in mind that with this option selected, it can take a longer time to browse pages you have previously viewed.
- Every Time You Start Internet Explorer
    - When you return to a Web page viewed in a previous session, Internet Explorer will check for updates to the page. Selecting this option can improve performance when viewing Web pages you have viewed previously.
- Automatically
    - When you return to a Web page viewed in a previous session, Internet Explorer will check for updates to the page. However, if Internet Explorer determines that a Web page rarely changes, it will check for updates less frequently. This option provides the best performance when you are browsing Web pages.

- Never
  - Internet Explorer will never check for updates to Web pages you have previously viewed.

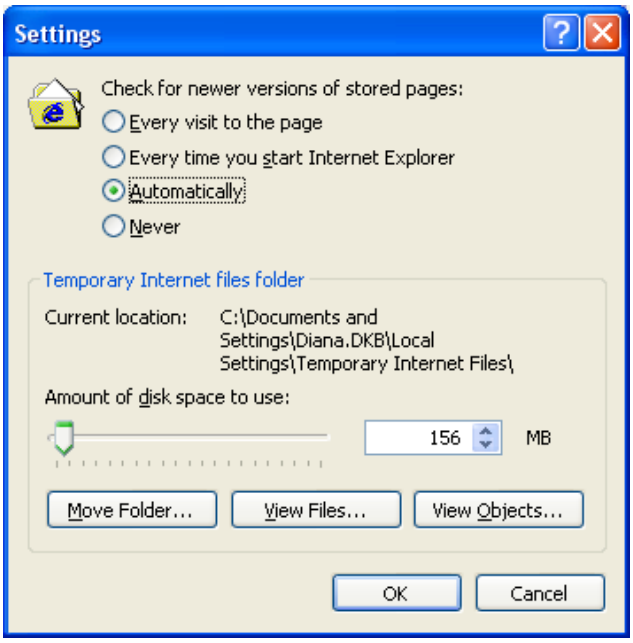

Figure: Configuring temporary internet files settings

The amount of disk space allocated to the Temporary Internet Files folder can be increased or decreased. Be aware that if you configure a value that is too low or too high, you may experience a decrease in performance. For example, if the value is too high, your hard disk may be filled up with outdated Web information. Setting the value too low may increase the amount of time it takes Internet Explorer to display Web pages. When the maximum amount of disk space allocated to the Temporary Internet Files folder is reached, older files are removed to make room for new content.

You can adjust this setting from the General tab of the Internet Options dialog box. Click the Settings button and type the new maximum size of the temporary Internet files folder.

The folder can also be moved if your computer is configured with multiple volumes. Click the Move Folder button from the Settings dialog box and browse to the new location. By default, the folder is stored on the same volume that Windows XP is installed on.

Another option you have for configuring the Temporary Internet Files folder settings, is to have the contents of the folder deleted automatically. You can configure this setting by following the steps listed below:

1. Open Internet Explorer.
2. Click Internet Options from the Tools menu.
3. On the General tab, you will see that you can manually delete the files in this folder. Click the Advanced tab.

4. From the list of settings, select the Empty Temporary Internet Files Folder When Browser Is Closed check box. This option is located under the Security section.
5. Click OK.

Security Settings

For security purposes, Internet Explorer allows you to place Web sites into different zones. There are Web sites on the Internet that can pose as a threat. For example, malicious Web sites could potentially exploit known or unknown vulnerabilities in the Web browser and run code on your computer. Placing such Web sites into a more restrictive zone reduces such risks.

Specific restrictions can be placed on Web sites based on the zone. 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. By default, these sites have fewer restrictions than sites in the Internet zone.
Trusted Sites	These are sites that you trust not to damage your computer and/or data. By default, sites added to the Trusted Sites zones have almost no restrictions.
Restricted Sites	These sites are considered potentially harmful to your computer and/or data. By default, sites added to the Restricted Sites zone are heavily restricted to minimize security risks.

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.

Each security 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. Although, keep in mind that the point of using zones is so you do not have to configure security settings.

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 can create 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.

Privacy Settings

A cookie is a small text file that is stored on your computer's hard drive by a Web server. The text file stores personalized information about your visit to a web site. The Web server can then read the text file the next time you return to the website and use the information to deliver personalized content. For example, there are several websites that deliver the latest news stories, but deliver local news when you access their site. Or those sites that provide you with the local weather forecast for your area.

You should also know the difference between a first-party cookie and a third party-cookie. A first-party cookie is used to store information for the website you are currently viewing. Whereas a third-party cookie originates from a website other than the one you are currently viewing. For example, the Web site you are currently viewing may use third-party websites for advertising, and these sites may in turn use cookies. Third-party cookies are considered a privacy risk because they can be used by advertisers to track your actions across multiple, different Web sites. First-party cookies can only be used to track your actions on a single Web site.

Cookies are stored on your computer's hard drive. They are stored in a folder called Temporary Internet Files. You can find this folder in the c:\documents and settings\\<*username*>\local settings directory. You can easily identify which files in this folder are cookies because the name looks similar to the following: Cookie:username@website.com

A cookie can be deleted directly from within the Temporary Internet Files folder. It is much easier though to do so through Internet Explorer. The process is described below:

1. Open Internet Explorer, click Tools, and select Internet Options.
2. The Internet Options dialog box will appear.
3. If you want to delete all the cookies in the Temporary Internet Files folder, click the Delete Cookies button available from the General tab.
4. If you want to delete a single cookie, click the Settings button, and click the View Files button as shown in the figure.
5. This opens the Temporary Internet Files folder from where you can highlight a specific cookie and delete it.

Privacy settings in Internet Explorer allow you to control how cookies are handled on your computer. You have a number of different options from allowing all cookies to blocking all cookies. Internet Explorer has five different privacy levels to choose from.

- **Block All Cookies**: All cookies from all Web sites will be blocked. Any existing cookies on your computer will not be available to the Web sites that created them.
- **High**: Cookies without a compact privacy policy or those with a policy that uses your personal information without your consent are blocked. Cookies that were already on your computer before you installed Internet Explorer 6 can only be read in the first-party context.
- **Medium High**: Third-party cookies without a compact privacy policy or those with a policy that uses your personal information without your consent are blocked. First-party cookies without a compact privacy policy or those with a policy that uses your personal information without your consent are blocked. First-party cookies that do not have a compact privacy policy and cookies that were already on your computer before you installed Internet Explorer 6 can only be read in the first-party context.

- **Medium:** Third-party cookies without a compact privacy policy or those with a policy that uses your personal information without your consent are blocked. First-party cookies that have a compact privacy policy, which specifies that personally identifiable information is used without your implicit consent, are allowed but deleted when you close the browser. First-party cookies that do not have a compact privacy policy are only readable in the first-party context. Cookies that were already on your computer before you installed Internet Explorer 6 are also only readable in the first-party context.
- **Low**: First-party cookies that do not have a compact privacy policy can only read the first-party context along with those cookies that existed before upgrading to Internet Explorer 6. Third-party cookies that do not have a compact privacy policy, or that have a compact privacy policy that specifies that personally identifiable information is used without your implicit consent, are deleted when the browser is closed.
- **Accept All Cookies**: All cookies are permitted.

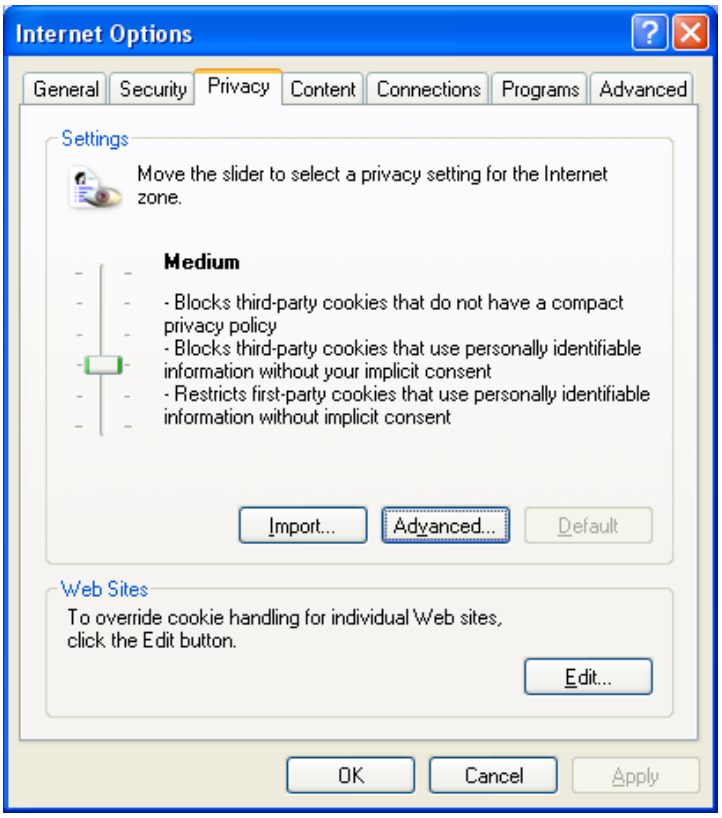

Figure: Internet Explorer privacy levels

By default, the privacy level in Internet Explorer is set to Medium. This means that Internet Explorer places some restrictions on the use of cookies, such as it blocks certain third-party cookies. You can customize the privacy level to suit your needs using the following steps:

1. Open Internet Explorer.
2. Click Tools and select Internet Options.
3. Click the Privacy tab shown in the following figure.
4. Move the slider up or down to change the privacy level.

When you are customizing the privacy level, if you move the slider to block all cookies, you may not be able to view some Web sites or take advantage of personalized features.

Internet Explorer also allows you to manage cookies on a per-site basis. Any site-specific settings you configure will override the privacy level configured on the Privacy tab (unless Allow All Cookies or Block All Cookies is selected). You can use the steps outlined below to configure per site privacy actions.

1. Open Internet Explorer.
2. Click Tools and select Internet Options.
3. Click the Privacy tab and click the Edit button.
4. From the Per Site Privacy Actions dialog box, type in the address of the Web site you want to manage.
5. Click the Allow button to allow cookies from the Web site. Conversely, click the Block button to block all cookies from the Web site.
6. Click OK.

For more advanced users, you can override how the privacy level configured automatically handles cookies. For example, you may choose to allow all first-party cookies. You can configure the advanced settings by clicking the Advanced button from the Privacy tab within the Internet Options dialog box. The Advanced Privacy Settings dialog box allows you to Accept, Block, or Prompt first-party and third-party cookies. A word of caution again, if you use the Prompt option, the prompts you receive indicating that a Web site is trying to copy a cookie to your computer may become excessive.

Once you have configured your privacy settings in Internet Explorer, you may decide you want to disable access to those settings so no one else can make changes to them. This requires you to edit the local group policy:

1. Open the Start menu and click Run.
2. Type gpedit.msc in the Open field and click OK.
3. Navigate to the following location within the Group Policy Tree: User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel.
4. Double-click the Disable The Privacy Page policy and select the Enabled radio button.
5. Click OK.

Content Settings

Certain Web content may be considered inappropriate in a business or home environment. Internet Explorer uses the Content Advisor to control the type of Web content that is acceptable for viewing. As long as Web sites have a security rating, it can be blocked if the content is considered unacceptable.

Some Web sites require a user to verify their identity. In other words, they have to prove that they are who they claim to be. This is the purpose of digital certificates. They verify the identity of a user or computer.

Your browser also uses SSL (Secure Sockets Layer) certificates, which are used by your browser to verify the security of a Web site. For example, SSL certificates are used to verify that a Web site is properly identifying itself.

There are three buttons available for certificates from the Content tab for certificates. The Clear SSL State button clears any client authentication certificates from the SSL cache (normally, these certificates remain in the cache until the computer is restarted). You can use the remaining two buttons, Certificates and Publishers, to view the certificates currently stored on the computer and the certificate publishers that your computer trusts.

The Content tab includes two additional buttons: AutoComplete and My Profile. With AutoComplete, Internet Explorer can display possible Web site matches based on what has been typed into the address bar. The AutoComplete Settings enable you to specify what you want to use AutoComplete for. Because someone can use the AutoComplete feature to identify Web sites that you have previously visited, you have the option of clearing the AutoComplete history.

Using the My Profile button, you can create a personal profile that stores information such as your name and address. When a Web site requests such information, it can get it from your personal profile (with your permissions), instead of you having to manually provide it.

The Profile Assistant is enabled by default in Internet Explorer. However, if you do not want any of your personal information shared with Web sites, you can disable this feature. To do so, select the Advanced tab from the Internet Options dialog box and clear the Enable Profile Assistant option.

Connection Settings

Internet Explorer connection properties are used to configure how the Web browser will connect to the Internet. The Connections tab lists any Internet connections currently configured on the computer, including dial-up and Virtual Private Network (VPN) connections.

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
  - If a network connection is not detected, Internet Explorer will attempt to connect to the Internet using the default dial-up connection.
- Always dial my default connection
  - Internet Explorer will always attempt to connect using your default dial-up networking connection.

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. Provide the address and port number of the proxy server. By selecting the Advanced 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 for computers on your local intranet. When accessing computers on the exception list, the proxy server is not used.
Bypass Proxy Server 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.

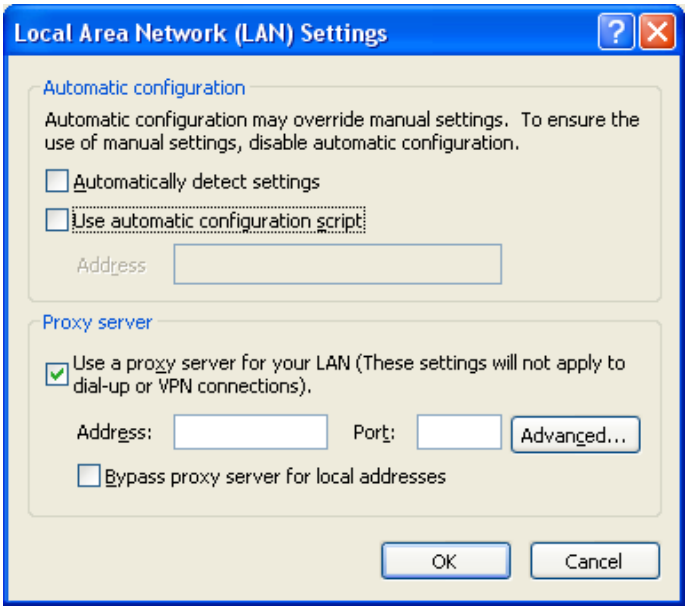

Figure: Configuring Internet Explorer connection settings

Programs Settings

If you are using only a single browser, that is the program that will be launched when you click an HTML file, type in a URL from the run command, and so on. However, if you are using more than one browser, you may have a preference as to which one is the default. A user can configure Internet Explorer to be their default browser by opening the Internet options dialog box (Tools | Internet Options). From the dialog box that appears, click the Programs tab. Place a check beside the option at the bottom of the box "Internet Explorer should check to see whether it is the default browser."

The settings on the Programs tab also determine the programs that Windows will invoke by default for specific Internet services. For example, a user can change the default email program that is used by Internet Explorer. When you click an email link on a Web page, that is the email client the Internet Explorer will automatically open. To change the current email program, open Internet Explorer, click the Tools menu and click Internet Options. From the Internet Options dialog box, click the Programs tab. Use the drop down arrow beside the E-mail to select the program you want Internet Explorer to use. Click OK.

One extremely useful new feature for Internet Explorer that is added with the installation of SP2 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 lists all the third-party add-ons installed in Internet Explorer, and it allows you to disable them individually.

Advanced Settings

There are various settings that can be configured from the Advanced tab of the Internet Options dialog box. The categories of settings that can be configured are described in the table below.

Setting	Description
Accessibility	Accessibility settings are designed for users with disabilities.
Browser	The browser settings are used to control how Internet Explorer behaves when you are viewing Web sites.
HTTP 1.1 Settings	Specifies whether Internet Explorer uses HTTP 1.1. These settings should not be enabled if a Web site uses HTTP 1.0.
Microsoft VM	These settings tell Internet Explorer how to handle Java applets.
Multimedia	These settings tell Internet Explorer how to handle multimedia files on Web sites.
Printing	Tells Internet Explorer whether or not to print background colors and images.
Search from the Address Bar	These settings customize the way Internet Explorer performs searches from the address bar when enabled to do so.
Security	These settings enable you to configure Advanced security settings to help protect your computer and data when accessing the Internet.

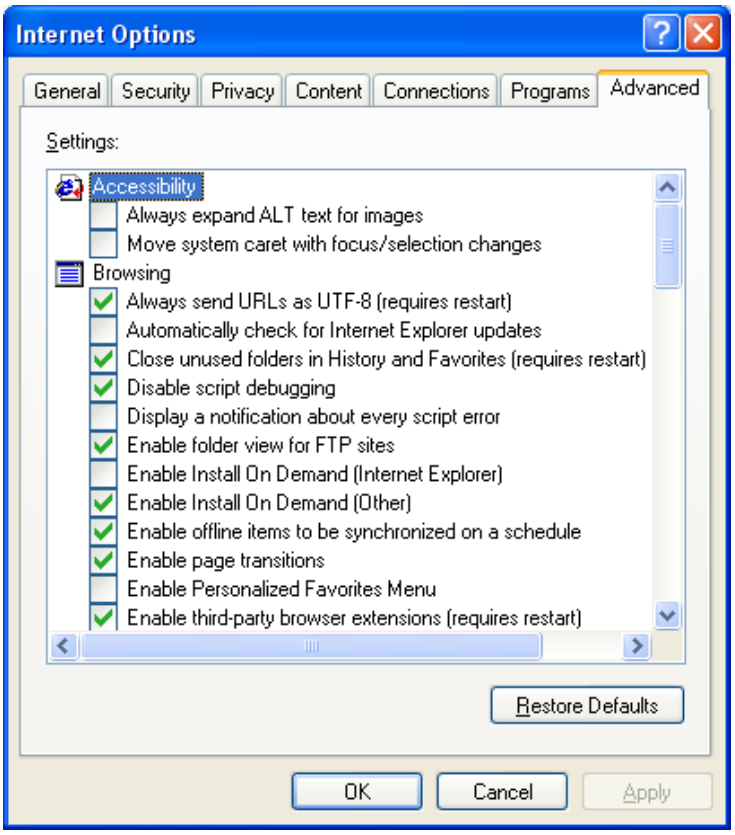

Figure: Internet Explorer Advanced settings

Configure and troubleshoot Outlook Express

Configure and troubleshoot news reader account settings

Newsgroups allow people to easily share information. A newsgroup server usually hosts several newsgroups. Once you connect to a news server, you can select which newsgroups you want to be a member of. A single newsgroup will normally be dedicated to a specific topic.

The first step in setting up newsgroups in Outlook Express is to connect to the news server.

1. Within Outlook Express, Select Tools, and click the Accounts option.
2. From the Internet Accounts dialog box click the News tab.
3. Click the Add button and select News.
4. Type your name and click Next. This is the name that will appear when you post messages to a newsgroup.
5. Type your email address and click Next.
6. Enter the name of the news server supplied by your ISP or network administrator. If the news server requires credentials, select the My News Server Requires Me to Log On option. Click Next.

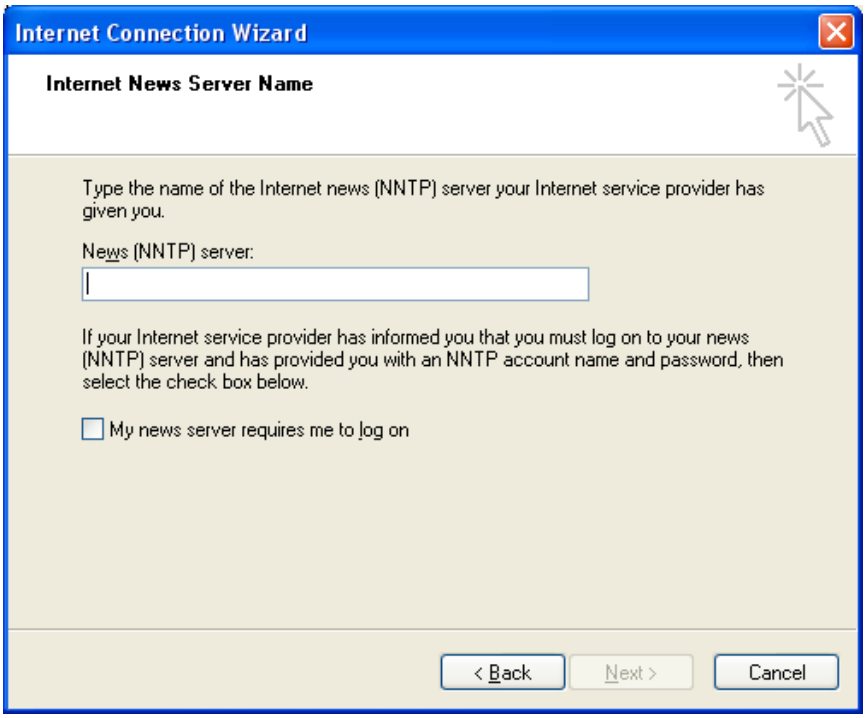

Figure: Specifying the name of the news server.

7. If you selected the My News Server Requires Me to Log On option, type in the user account name and password that will be used to access the news server. Click Next.

8. Click Finish.

Once the news server has been added, a user can then pick the newsgroups on the news server that they want to subscribe to. A user can subscribe to a newsgroup by completing the following steps.

1. Within Outlook Express, select the news server you have added under the folder list. A window appears informing you that you have not subscribed to any newsgroups.
2. Click Yes to subscribe now.
3. The Newsgroups Subscriptions dialog box appears and displays all the newsgroups available on the news server. Select a newsgroup of interest and click the Subscribe button.
4. Repeat step 2 for any additional newsgroups you want to subscribe to. The newsgroups you subscribed to are displayed in Outlook Express.
5. To read the messages posted to a newsgroup, click the name of the newsgroup. The messages are displayed in the right pane.

If a user is unable to connect to a news server, verify that they can successfully establish a connection with their ISP. You should also check the settings to verify that the user has entered the correct name of the news server and the correct port. Most news servers use port 119. If users are required to log on to the news server, make sure the correct username and password have been specified.

Another problem users may encounter is that they can connect to the news server but cannot view any newsgroups. In such cases, verify that the correct news account settings have been configured.

Configure and troubleshoot e-mail account settings

To create a new e-mail account in Outlook Express:

1. Click Start, point to All Programs, and select Outlook Express.
2. From the Tools menu, click Accounts. The Internet Accounts dialog box appears.
3. Select the Mail tab, click the Add button, and click the Mail option. This action launches the Internet Connection Wizard.
4. Type in a display name. This is the name that will appear on any outgoing messages. Click Next.
5. Type in the email address. This information will be provided by the network administrator or by the user's ISP. Click Next.
6. Use the drop-down arrow to select the type of incoming mail server: POP3, IMAP, or HTTP.
7. Type in the names of the incoming and outgoing mail servers. Click Next.
8. Type in the user name and password for the account. This information will also be available from a network administrator or the user's ISP. Click Next.
9. Click Finish to close the Internet Connection Wizard.

Outlook Express allows you to access your Web-based email. The process for setting up Outlook Express to check your Web-based email is slightly different than setting up your email account from an ISP. You can use the following steps to configure OE 6 to check a Web-based account.

1. Click Tools and select Accounts.
2. From the Mail tab, click Add, and select Mail.
3. Type in your display name and click Next.
4. Type in your email address, which will be your hotmail address.
5. From the Email Server Names dialog box, make sure HTTP is selected for the incoming mail server. The incoming mail server will be automatically filled in for you. Click Next.
6. Type in your hotmail address and password. Click Next.
7. Click Finish.

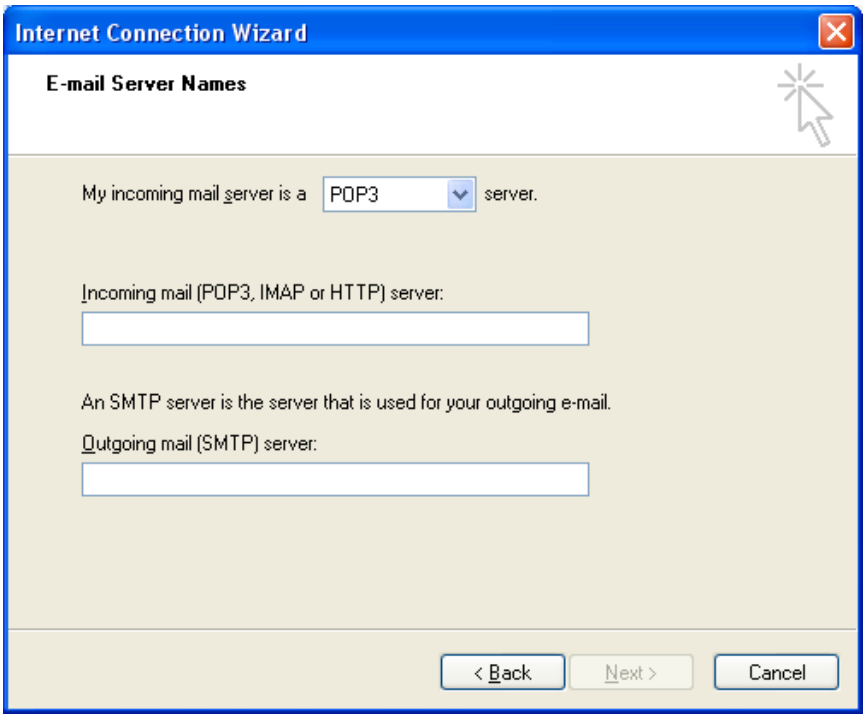

Figure: Specifying the name of the incoming and outgoing e-mail server

Once an email account is setup, you can configure it from the account's properties dialog box shown in the figure below.

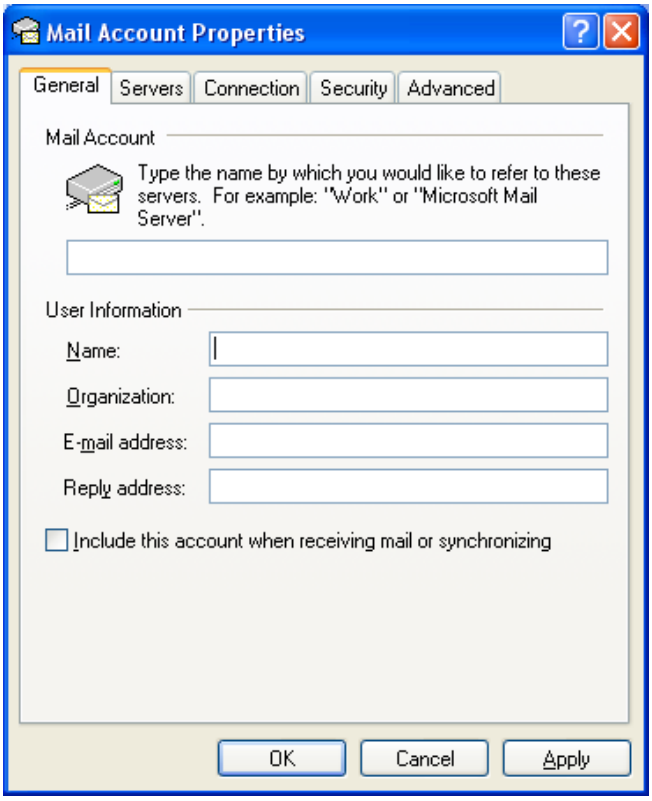

Figure: Configuring e-mail account settings

The General tab allows you to configure the user's name and e-mail address. You can also specify an alternate reply address. To have Outlook Express check for new messages, select the Include This Account When Receiving Or Synchronizing option.

From the Servers tab, a user can change the name of the incoming and outgoing mail servers as well as their credentials. The Connection tab is used to configure how Outlook Express will connect to send and receive messages. If you do not select the Always Connect to This Account Using option, Outlook Express connects to the Internet using the settings configured in Internet Explorer. Conversely, you can override the settings in Internet Explorer and specify the dial-up or LAN connection Outlook Express should use to connect to the Internet.

Digital certificates verify that you are who you say you are. If you have been assigned a digital certificate, you can use it to digitally sign all your outgoing messages. You can configure the signing certificate and encrypting preferences for an email account using the Security tab.

Finally, there are numerous settings on the Advanced tab that are described in the table below.

Setting	Description
Outgoing Mail (SMTP)	Configure which port on the outgoing mail server to connect to. The default value is port 25.
This Server Requires a Secure SSL Connection	Specifies whether to use the Secure Sockets Layer protocol. This option can be enabled for outgoing and/or incoming mail servers.
Incoming Mail (POP3)	Configure which port to connect to on the incoming mail server. The default value is port 110.
Server Timeouts	Configure how long Outlook Express should wait for a response from the mail server when attempting to send or receive messages.
Break Apart Messages Larger Than	Tells Outlook Express to break apart messages larger than the value specified. This option is available because some older mail servers are unable to handle messages larger than 64KB.
Leave a copy of messages on server	Specified that a copy of all received messages should be left on the mail server. This option appears only for POP accounts.
Remove from Server After	Specifies when messages stored on the incoming mail server should be deleted. This option appears only for POP accounts.
Remove from Server When Deleted from 'Deleted Items'	Specifies that messages deleted from the Deleted Items folder are also deleted from the mail server. This option appears only for POP accounts.

As a Desktop Support Technician, you have to be able to troubleshoot common problems that occur in Outlook Express. The error message that a user receives when they are trying to send or receive e-mail will be a good indication as to what the problem is.

You can use the following points when troubleshooting Outlook Express:

- Verify that the computer has Internet or LAN connectivity.
- Make sure the user has entered the correct credentials.
- Check to see that the e-mail account settings match those of the mail servers.
- Increase the server timeout value if the user continuously receives a timeout message.

Configure the operating system to support applications

Configure and troubleshoot file system access and file permission problems on multi-boot computers

It is possible to run two operating systems on a single computer. For example, you may have both Windows XP and Windows 95 installed on one computer. In a multi-boot configuration, you will be presented with a boot menu during computer start up from which you can choose which operating system to start. If you are multi-booting Windows XP with another version of Windows, the general rule of thumb is to install the earlier version first. Using the previous example, Windows 95 would therefore be installed on the computer first. You can then proceed to install Windows XP on a separate volume.

If you are multi-booting Windows XP and Windows 2000, Windows XP should be installed after Windows 2000 has been installed. All non-Microsoft operating systems and earlier versions of Windows should be installed first. As an example, if you plan to install Windows XP and Windows 98, Windows 98 should be installed first.

You need to consider compatibility issues when multi-booting. If you are multi-booting Windows XP with an older platform such as Windows 95, you must think about file system issues. When you install Windows XP, you can use either FAT or NTFS. What you need to keep in mind is that NTFS is not supported by all operating systems. Therefore, any partitions that are formatted with NTFS may not be accessible when you boot under another operating system. For example, any NTFS partitions on the local computer will not be readable under Windows 95.

Yet another point to consider is basic and dynamic disks, which were introduced with Windows 2000. Pre-Windows 2000 operating systems do not support dynamic disks. When multi-booting any of pre-Windows 2000 platforms with Windows XP, they must be placed on a basic disk that is formatted with FAT. Also, any dynamic disks on the local computer will not be readable under these older versions of Windows.

Configure access to applications on multi-user computers

The Start Menu can be customized so the same programs are available to all users that log on. For example, if a computer is shared amongst multiple users that all require access to the same group of programs, you can create a submenu off the Start Menu that will be available regardless of which user logs on. To customize the Start Menu for all users:

1. Right click the Start button and select Open All Users.
2. Open the folder in which you want to create the submenu.
3. Click File, point to New and click Folder.
4. Type in a name for the folder and press Enter.
5. Drag any programs or items you want to appear on the submenu into the folder just created.
6. These changes will now appear on the Start Menu regardless of the user logged on.

Most setup procedures give you the choice of installing an application for a single user or for all users. In a multi-user environment, the best thing to do is install the applications for all users.

If a computer is shared amongst multiple users, you can control who can run various applications that are installed. This is done by configuring permissions on an application's executable. Locate the appropriate executable within Windows Explorer. Open the properties dialog box for the executable and click the Security tab. Use the Add button to select the user account you want to configure permissions for.

By default, all users will have Read and Read and Execute permissions to an executable.

Resolving Issues Related to Application Customization

Resolve issues related to customizing an Office application

Customize toolbars

A user can customize the toolbars in any Microsoft Office application. The process is the same regardless of the application a user is in. From the View menu, point to Toolbars, click Customize, and select the Toolbars tab. Keep in mind that although the process is the same, each application will have its own specific toolbars and toolbar icons.

If a user is having a problem with a toolbar, be sure to open the troublesome application before troubleshooting the toolbar in question.

The Toolbars tab allows you to do the following:

- Enable and disable toolbars
- Create a new toolbar
- Rename an existing toolbar
- Delete custom toolbars
- Reset toolbar
- Assign a keyboard shortcut to a command

A user can also add specific buttons to a toolbar. This can be accomplished using the procedure below:

1. From the View menu, point to Toolbars, and click Customize.
2. In the Customize dialog box, click the Commands tab.
3. Under Categories, select the category from which you want to add the button.
4. To add a button to a toolbar, drag a button from the Commands list to the desired toolbar.

Configure proofing tools

There are numerous add-ins that are available for Microsoft Office. One such add-in is the Proofing Tools. It provides an additional collection of tools, such as spelling and grammar checkers, thesauri, and AutoCorrect lists, for more than 45 languages.

Microsoft Office comes with built-in proofing tools for commonly used languages. For example, the English version of Office includes proofing tools for French and Spanish, as well as English. By installing Office Proofing Tools, you add those same capabilities for many more languages. This makes it even easier to quickly and accurately enter and edit text in the languages you want, creating powerful, professional, and error-free documents.

When you install Office Proofing Tools, the following tools are added to most Office programs:

- Spelling checkers and their accompanying dictionaries
- Grammar and writing style checkers
- Thesauri for checking synonyms
- Hyphenators
- AutoCorrect lists
- AutoSummarize
- Input Method Editors (IMEs)
- Word breakers
- Simplified/traditional Chinese translator
- Tools for working with Korean text, such as Hangul Hanja converter and Hanja dictionary
- Additional bilingual dictionaries

Proofing Tools are available for purchase at www.shop.microsoft.com or a licensed reseller.

Although Microsoft Word has its own dictionary, it probably does not contain all the words and acronyms that you use. If this is the case, you can add your own frequently used words, acronyms, and names to the dictionary.

1. Open Microsoft Word.
2. From the Tools menu, click Options.
3. Select the Spelling and Grammar tab.
4. Click the Custom Dictionaries button.
5. Place a check beside the dictionary you want to modify.
6. Click the Modify button.
7. In the Word field, type in the word you want to add to the dictionary and click the Add button. Click OK.
8. Click OK to close the Custom Dictionaries dialog box.
9. Click OK to close the Options dialog box.

Conversely, if you want to remove a word from the dictionary, complete steps 1 through 7. Select the word you want to remove and click the Delete button.

When you open a new document, Word applies the font style, views, and so on found in the Normal.dot template. If you don't care for the formatting and other options configured in the template, they can be changed. However, before you can do this, you need to know how to find the Normal.dot template.

If you are new to Word and do not know where the template is located, you can use these simple steps to find out.

1. Open Word.
2. From the Tools menu, click Options.
3. Select the File Locations tab.

4. Under the list of File types, select User templates.
5. Note the path to where the templates are stored.

If the full path is not displayed, click the Modify button. Click the drop down arrow beside the Look In field. You can then note the location of the template. By default, the location should be c:\Documents and Settings\username\Application Data\Microsoft\Templates

The Normal template is used each time you open a new Word document. The template has pre-configured formatting such as font type and size that is automatically applied to each new document. What if the Normal template is not set up the way you want it to be? You could make the formatting changes each time or you can set up the Normal template exactly as you want it.

To change the Normal template:

1. In Windows Explorer, navigate to c:\Documents and Settings\username\Application Data\Microsoft\Templates.
2. Select Normal.dot.
3. From the Edit menu click Copy.
4. Click anywhere within the templates folder and click Paste from the Edit menu.
5. Right-click the existing Normal.dot file and rename it to anything you want.
6. Right-click the copy you made and rename it to Normal.
7. Right-click the new Normal template and click Open. DO NOT double-click the template. This will open a new document.
8. Within the template, make the changes you want. This includes font size and style, toolbars, views and so on.
9. From the File menu, click Save.

Word will now open new documents using the template you just created. You can always revert back to the old template by renaming it back to Normal.dot.

Manage Outlook data, including configuring, importing, and exporting data, and repairing corrupted data

Outlook allows you to import and export data. The Export feature copies the specified data intact to a file, while the Archive feature only copies old data to the Archive file.
To Export data in Outlook:

1. Open Outlook and click on File, select Import and Export.
2. The Import and Export Wizard will start. Select "Export to a file" and click Next.
3. Select "Personal Folder File (.pst)." Click Next.
4. Select "Personal Folders" at the top of the dialog box to back up all of your Outlook data. Make sure that the check box labeled Include Subfolders is checked. Click Next.
5. Select a destination for the folder.
6. Outlook labels the backup file "backup.pst", and you can set the destination by placing the drive letter before the destination file name. For example, if your Zip drive is drive E:, you would just type "E:\backup.pst" (without the quotes). It's a good idea to select "Do not export duplicate items" in the Options box.
7. Click Finish and your Outlook data will be exported.

If a user is unable to import a PST file, there is a good chance that it is corrupt. The Inbox Repair Tool can be used to repair a corrupt PST. The tool works by repairing the file's header and then deleting any information that it does not recognize. The Inbox Repair Tool (Scanpst.exe) is located in the drive:\Program Files\Common Files\System\MSMapi\1033\ directory of any system that is running Windows XP.

Resolve issues related to customizing Outlook Express

Most software usually allows you to customize different features and Outlook Express is no exception. Users can customize a variety of settings from the interface to how Outlook notifies them of new messages.

Outlook Express Toolbar

One of the most common things a user can customize in Microsoft applications, such as Internet Explorer, Word, Outlook, and so on is the toolbar. Users can customize the toolbar in Outlook Express to meet their personal needs.

To do so, click the Layout option from the View menu. If you click on the Customize Toolbar button, you can configure which buttons you want visible. To add a button, simply highlight it from the list of available buttons and click Add. Once you are done, click Close.

Once you are back at the Windows Layout Properties dialog box, you can customize the basic layout of Outlook Express by specifying which components you want visible. You can also configure how you preview your messages under the Preview Pane section.

Importing and Exporting Data

Mail messages can be imported to and exported from Outlook Express using the respective commands. To export mail messages in Outlook Express:

1. Click File, point to Export, and select Messages.
2. Click OK.
3. In the Choose Profile dialog box, select the program you want to export your mail messages to (for example, Microsoft Outlook).
4. From the Export Messages dialog box, select the folders you want to export and click OK.

To import messages into Outlook Express:

1. Click File, point to Import, and select Messages.
2. Select the email program you want to import your messages from and click Next.
3. Select the folders you want to import into Outlook Express and click Next.
4. Then click Finish.

Outlook Express Identities

Outlook Express can be configured to support multiple users who share a single computer. You can set up Outlook Express for multiple users without having to create multiple user accounts in Windows. This is done through Outlook Express identities. An identity in Outlook Express will have its own signature, accounts, address book and settings. For added security, you can also use passwords to protect an identity. You can create a new identity in Outlook Express using the following procedure:

1. Open Outlook Express.
2. Click File, point to Identities, and click Add New Identity.
3. In the Type your name field, enter the name for the new user.
4. If you want to protect the identity with a password, place a check beside Require A Password. Type the password for the identity, and then click OK.
5. Click OK to close the New Identity dialog box.

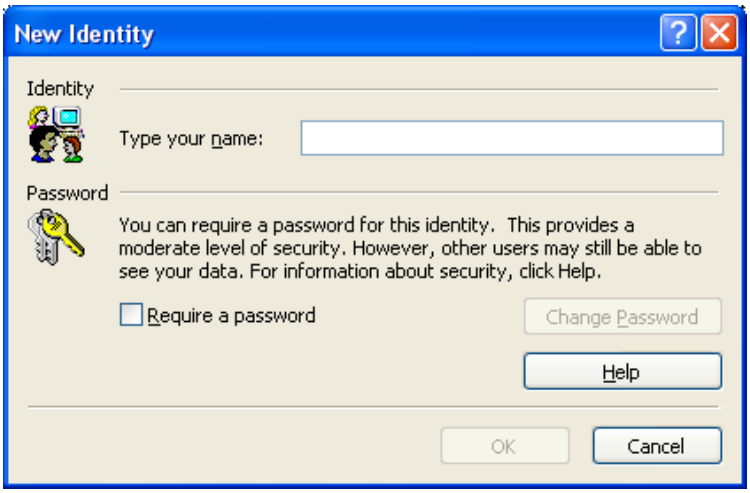

Figure: Creating multiple identities in Outlook Express

Block Senders

If you have an email address, you have more than likely found spam in your inbox at some point in time. Spam is what you would refer to as unwanted email, and there are a few ways in which you can keep it out of your inbox.

In Outlook Express, one of the ways in which you can prevent spam is to use the Block Senders feature. You have the option of blocking individual email addresses. Once a sender's email address has been blocked, you will no longer receive messages from them. However, spam often contains randomly generated sender email addresses, which makes blocking the sender impossible.

To block a sender, highlight an unwanted message within your Inbox, click the Message menu, and select the Block Sender option. A message appears informing you that the sender is blocked. Click Yes to confirm this action.

A more efficient approach instead of blocking an individual sender may be to block an entire domain. You can do this within Outlook Express by clicking the Tools menu, pointing to Message Rules, and clicking Block Senders List. From the Message Rules dialog box, make sure the Block Senders tab is selected and click the Add button. From the Add Sender dialog box, type in the domain name. You can then choose what you want blocked: mail messages, news messages, or both. Click OK. Click OK to close the Message Rules dialog box. Now when a message from the domain is sent to you, Outlook Express will automatically delete the message.

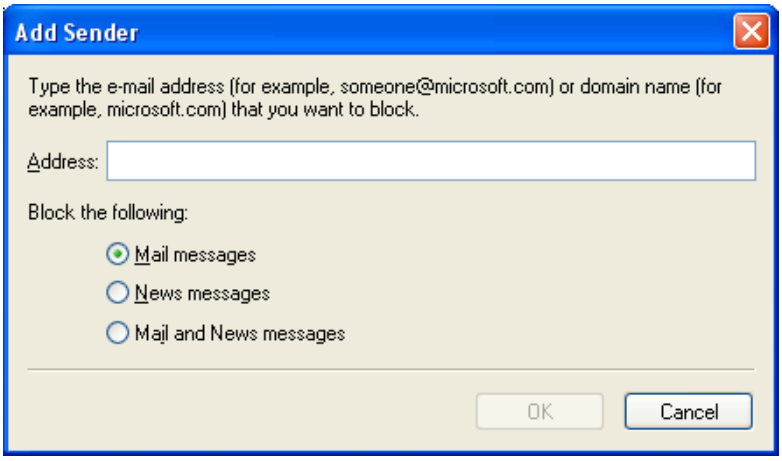

Figure: Blocking a domain in Outlook Express

Blocking HTML Content

Most people use e-mail on a regular basis. You may have noticed that some HTML messages (particularly spam) contain references such as images that are located on their Web servers. In the past, when you opened such a message, Outlook Express would automatically contact the Web server to display the information. The problem with this is that when Outlook Express retrieves the information, the Web server can identify you as the recipient and thereby once again increase the amount of spam you will receive in your inbox.

Once you install SP2 on Windows XP, Outlook Express includes an option that will block external HTML content that is received in e-mail messages. It is generally a good idea to have this option enabled so you can protect your privacy. You can verify that this option is indeed enabled, using the steps outlined below:

1. Open Outlook Express.
2. From the Tools menu, click Options.
3. Select the Security tab.
4. Place a check beside Block Images And Other External Content In HTML E-mail.
5. Click OK.

Sending Messages

Users can customize when Outlook Express sends the messages they have composed. One option is to change your default settings in Outlook Express so that messages are not sent automatically when you press the Send button. Instead, messages are placed in your Outbox until you hit the Send/Recv button. You can configure this option within Outlook Express by selecting Options from the Tools menu. Click the Send tab and clear the box beside the option to Send messages immediately as shown in the figure.

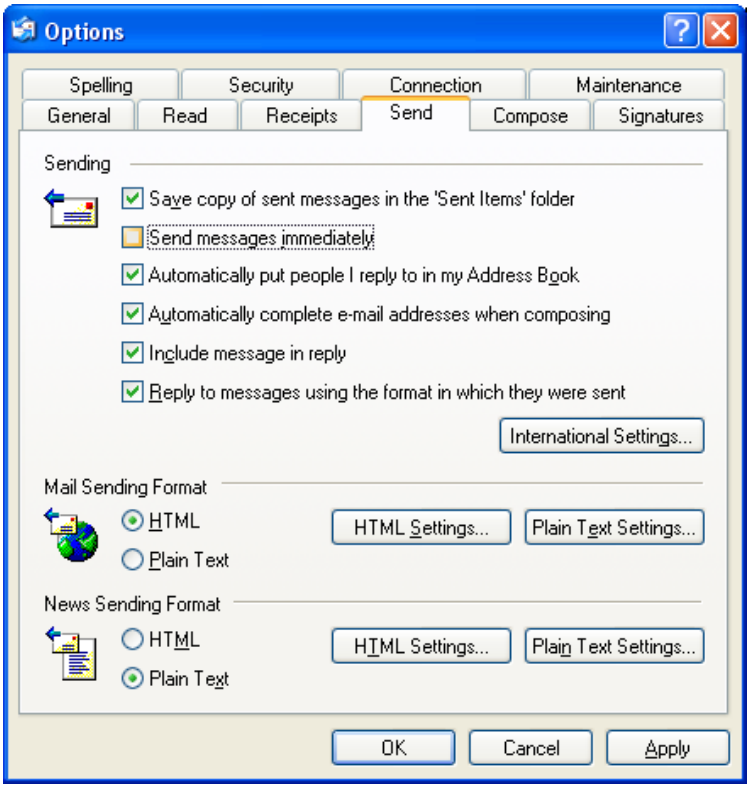

Figure: You can configure Outlook Express to place your e-mail in the Outbox till you are ready to send.

Once you compose your e-mail and press the Send button, you will receive a message that your e-mail will be stored in your Outbox.

Another option you have that does not require you to make any configuration changes within Outlook Express is to save your e-mail to the Drafts folder. After you compose your message, simply click File then Save As. When you are ready to send the e-mail, you can open up your Drafts folder and send the message.

Managing E-mail Messages

Outlook Express mail rules are a great way of keeping your emails organized. If you receive a high volume of email messages, you may want to change the way Outlook Express processes them. For example, you may want messages from a specific person to be sorted and placed into a specific folder or highlighted in a different color.

By creating rules in Outlook Express, as shown in the following steps, you can change how incoming mail messages are processed:

1. Within Outlook Express, click the Tools menu option, point to Message Rules, and click Mail.
2. Select one or more conditions for the rule. For example, if you select Where the From Line Contains People, the mail message must be from a specific person before any processing actions are performed.
3. After you have specified the conditions, you must edit the value for each condition by selecting the hyperlink under Rule Description.
4. Specify the actions for the rule. Outlook Express will take these actions if a mail message meets all the conditions.
5. Edit the values for the actions by selecting the hyperlink under Rule Description. For example, if you select the rule Move It To The Specified Folder, you then have to edit the value of the rule and tell Outlook Express which particular folder mail should be placed in.
6. Type a descriptive name for the rule.
7. Click OK.

Outlook Express does not have a backup function. However, if you use Outlook Express as your email client you may want to backup your messages in the event that you need to restore them. The process is not as simple as it is in Outlook but it is certainly something you should consider doing.

Before you can make a copy of your messages, you must first compact them.

1. Open Outlook Express.
2. Click File, point to Folder, and click Compact All Folders.
3. A window will appear informing you that it is compacting.
4. Once complete, your folders are saved to a file with a .dbx extension.

Next, you have to locate the correct file (with the .dbx extension) and make a copy of it.

1. Open Windows Explorer to search for the files with a ".dbx" extension.
2. In your search box type *.dbx, Windows will search for all files with this extension.
3. You may have several files appear. You want to backup the most recently modified. You can determine this by checking the date modified field.
4. Once you've identified the correct file, make note of the path.
5. Browse to the file in Windows Explorer.
6. Right-click the Outlook Express folder and click copy.
7. Paste the folder in the location where you want to store the folder, such as a CD or zip drive.

Security Zones

Security zones in Outlook Express determine whether active content can be run from within an HTML message. You can configure the security zone for Outlook Express using the following steps:

1. Click Start and select Outlook Express.
2. Within Outlook Express click the Tools menu and click Options.
3. From the Options window, select the Security tab.
4. Under Virus Protection, select Restricted Sites Zone. This option should be selected by default in Outlook Express 6. Previous versions of Outlook Express used the Internet zone, which is less secure because it allows most active content to run.

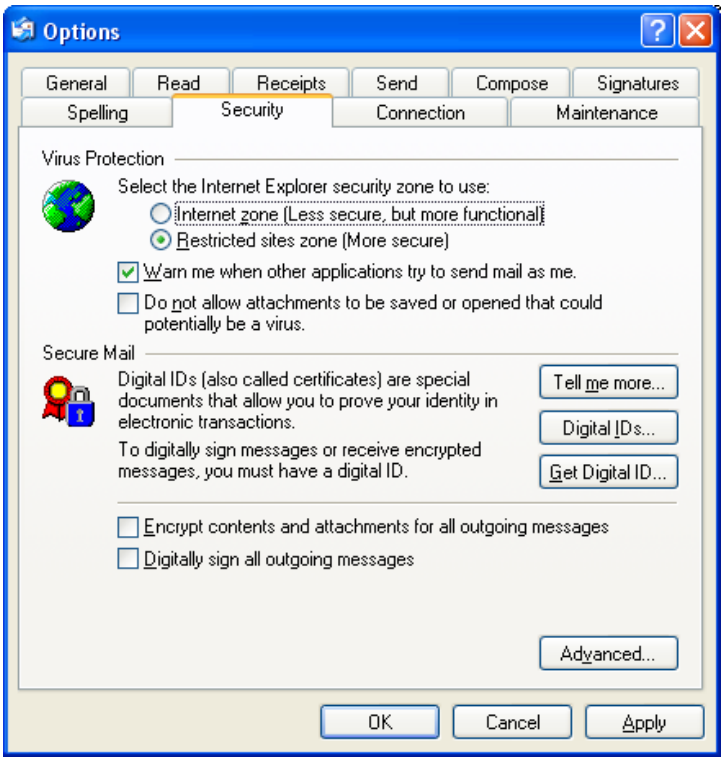

Figure: Configuring security zones in Outlook Express

Resolve issues related to customizing the operating system to support applications

Customize the Start menu and taskbar

The Start Menu displays the programs available on a computer. The Taskbar contains shortcuts to various programs. When you click the Start button, a list of programs and tools installed on the computer is displayed. Clicking any of the options launches a specific program.

The Taskbar is the bar displayed along the bottom of the desktop. It serves many purposes, such as fast switching between open programs. Every open program displayed an associated button on the Taskbar making it easy for a user to switch between programs. The active button on the Taskbar is the active program on the desktop. The Taskbar also contains the Start button, the Quick launch area, and the notification area.

Both the Start Menu and the Taskbar can be customized. Even if a computer is shared between multiple users, each user can customize these components to meet their own specific needs and preferences.

Customizing the Taskbar

To customize the Taskbar right-click the Start button and click the Properties option. This opens the Taskbar and Start Menu Properties dialog box. Select the Taskbar tab to configure related settings.

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	The taskbar is always visible.
Group Similar 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 Taskbar tab is also used to configure the Notification area. The Notification area is located beside the system clock in the bottom corner of the desktop. Notification area settings include: Show the clock and Hide inactive icons.

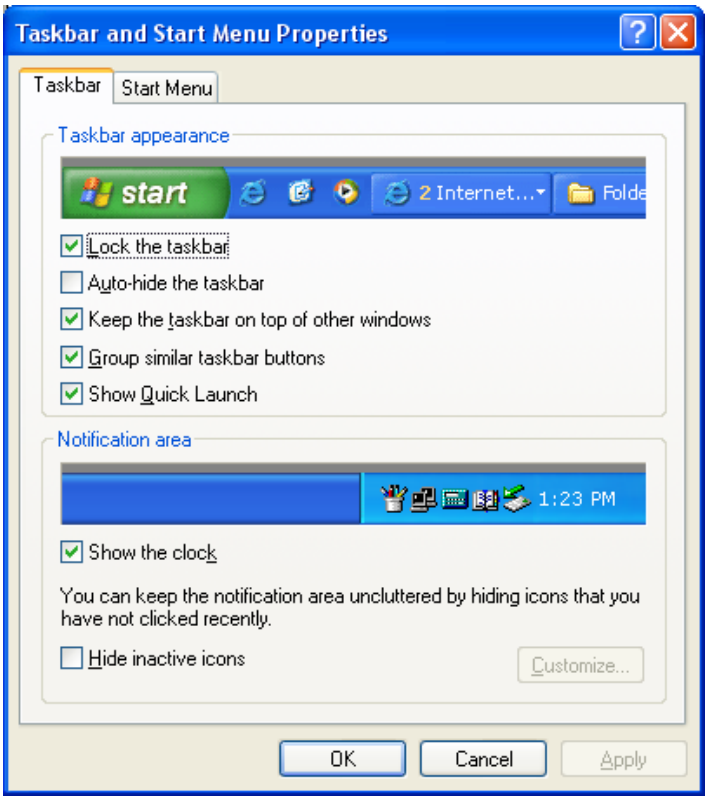

Figure: Configuring the taskbar

Customizing the Start Menu

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. The recently used 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 onto 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.

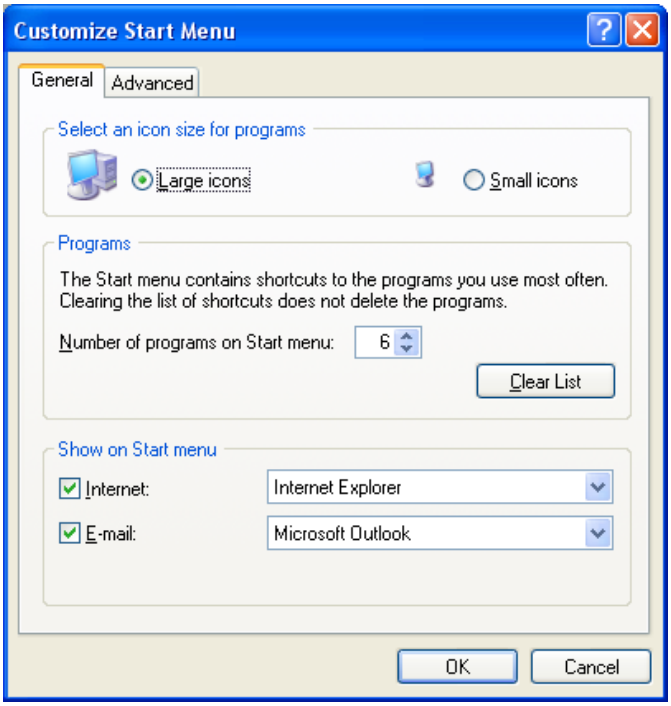

Figure: Configuring the StartMenu

The General tab allows you to configure the following settings:

- The size of icons displayed for programs.
- The number of programs that should appear on the frequently used list.
- The programs to Internet and E-mail programs to display on the Start Menu.

The Advanced tab allows you to configure the settings described in the table below.

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.

One point to remember is that any changes made to the Start Menu and Taskbar settings are only applied to the user that is currently logged on.

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 there 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. Corporate environments often want to restrict what configuration changes users can perform on their computer for security and stability purposed.

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 perform.

The Start Menu can be customized for an individual user or for all users that log onto the computer. To customize the Start Menu, right-click the Start button and click Open All Users. Conversely, to customize the Start Menu for a specific user, right-click the Start button and click Explore All Users. Open the folder for the users you want to customize the Start Menu for.

Customize regional settings

Windows XP can display information such as numbers and currency in different formats. It is the Regional Settings that tell Windows XP and different programs how to display information such as numbers, currency, time, and date. Regional settings can be changed using the Regional and Languages Options utility within the Control Panel.

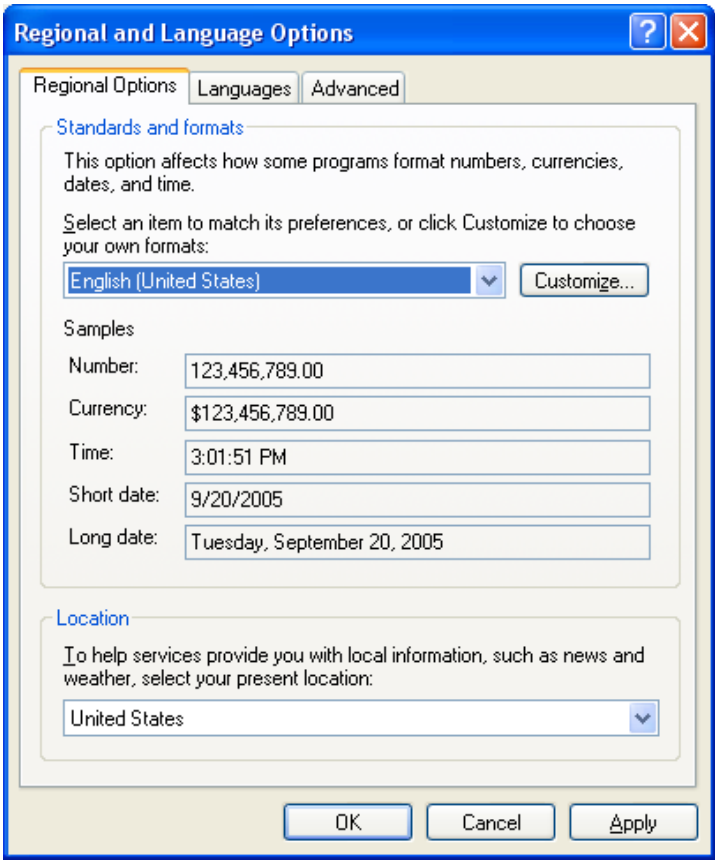

Figure: Configuring regional and language settings

Using the Regional Options tab, you can select your specific locale, such as English (United States). The locale will use preconfigured formatting for the options shown. Using the Customize button, you can manually configure how the different regional options will be displayed.

Customize fonts

The Fonts applet within the Control Panel lists all the fonts that are currently installed on a computer. When a new program is installed, it may come with its own fonts. For example, when you install Microsoft Office, it has its own fonts.

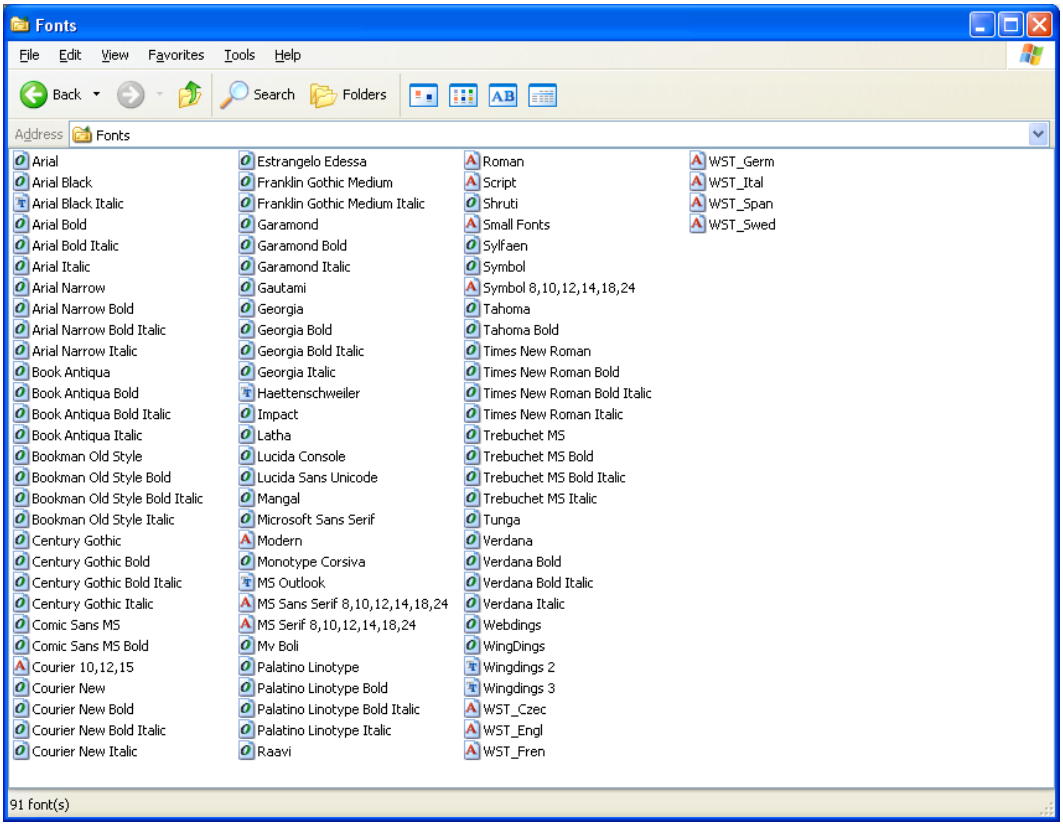

Figure: The Fonts applet lists all fonts installed on a computer

If a user requires a specific font that is not installed, you can install it using the Fonts applet.

1. Click Start and click Control Panel.
2. Double-click the Fonts utility. If the Fonts utility is not available, you must switch to Classic View.
3. From the File menu, click Install New Font.
4. Click the appropriate drive from the Drives list.
5. Double-click the folder that contains the new font.
6. Click the font you want to add and click OK.

Customize folder settings

There are fours tabs available from the Folder Options applet: General, View, File Types, and Offline Files.

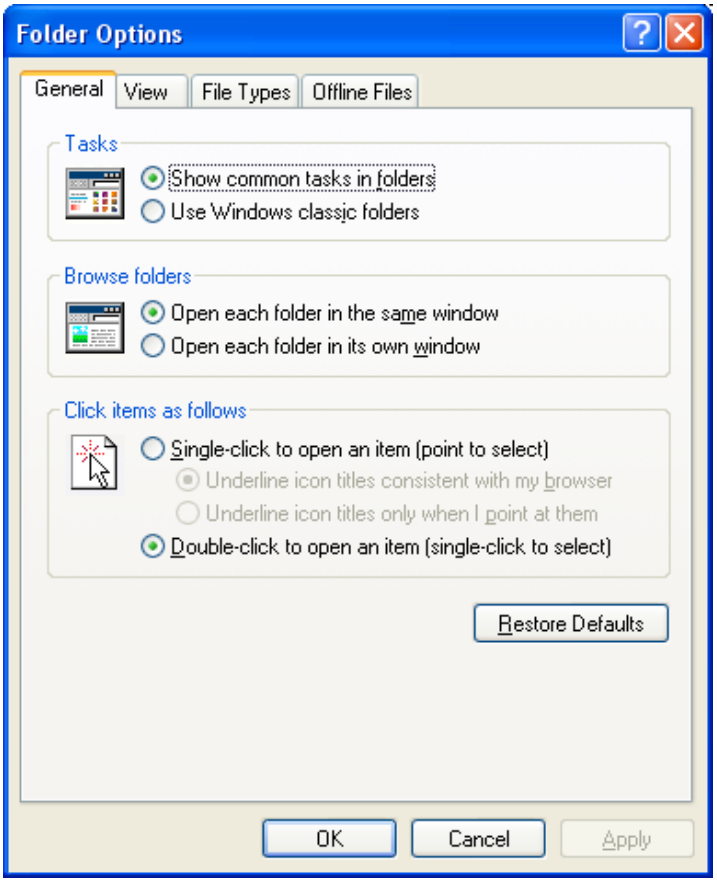

Figure: The Fonts applet lists all fonts installed on a computer

The General tab is used to configure the behavior and appearance of folders. Under the Tasks section, you can configure whether common folder tasks are displayed in folders. By default, common tasks are displayed in folders. By selecting the option to Use Windows classic folders, the list of tasks will not be displayed.

The General tab allows you to configure two additional options. You can have folders opened in the same window or in a new window. You can also change how folders are opened, with a single-click or a double-click.

The View tab allows you to reset all folders to the default settings and lists several advanced settings. Some of the settings are described in the table below.

Option	Description
Automatically Search For Network Folders And Printers	Windows will periodically search for the network for shared folders and printers and display them in My Network Places.
Display Simple Folder View In Explorer's Folders List	When a folder in the Folders List is selected, the contents and sub folders will be displayed. All other folders are closed when another folder is selected.
Display The Contents Of System Folders	The contents of system folders will be displayed. By default, the contents are hidden.
Display The Full Path In The Address Bar	The complete path to an open folder or file is displayed on the address bar.
Display The Full Path In The Title Bar	The complete path to an open folder or file is displayed on the title bar.
Do Not Cache Thumbnails	Folder thumbnails are not cached. This can increase the amount of time it takes to open folders that contain thumbnails.
Do Not Show Hidden Files And Folders	Program and system files will not be displayed in the file list for a folder.
Show Hidden Files And Folders	Program and system files will be displayed in the file list for a folder.
Hide Extensions For Known File Types	File extensions are not displayed.
Hide Protected Operating System Files (Recommended)	Operating system files will not be displayed in the list of files for a folder.
Launch Folder Windows In A Separate Process	Each folder is opened in a separate part of memory. This can increase stability but slow down performance.
Show Control Panel In My Computer	The Control Panel icon will be displayed in My Computer.
Show Encrypted Or Compressed NTFS Files In Color	Encrypted or compressed files and folders are displayed in different colors.
Use Simple File Sharing (Recommended)	Enables simplified sharing within a workgroup or network.

The File Types tab displays all the registered file types on the local computer. Each file extension listed is associated with a file type. You can use this tab to change the program that is used to open files with a specific extension.

Finally, the Offline Files tab is used to enable offline files and configure settings that apply to working with offline files. You can configure when offline files are synchronized, whether or not to encrypt offline files, and how much disk space is allocated to the storage of offline files.

Configuring and Troubleshooting Connectivity for Applications

Identify and troubleshoot name resolution problems

There are two ways that a DNS client can resolve hostnames to IP addresses. A static text file, called a Hosts file, can be used or a DNS server can be used. Everyone uses DNS, and you can use a Hosts file when you need to override DNS addresses, such as during troubleshooting.

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.
- The Hostname command can be used to display the hostname of the local computer. Hostname shows only how the local computer has been configured. Other computers may not be able to reach the computer by using the name displayed.
- 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 address and registered DNS names
    - IPCONFIG /FLUSHDNS - Empties the contents of the DNS cache

Identify and troubleshoot LAN and Routing and Remote Access configuration problems

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:

- Run diagnostics on the modem to verify that it is functioning correctly.
- Check that the modem is dialing the correct number for the remote access server.
- Make sure the user is providing the correct username and password.
- Verify that the remote access server is online.
- Make sure there are enough ports on the remote access server.
- If you are using remote access policies to control remote access connections, verify that the remote access policy is not prohibiting the connection.

Identify and troubleshoot network adapter configuration problems

When a user is experiencing network problems, one of the first things you should do is right-click the network adapter icon in the Network Connections utility and click Repair. In most situations, this procedure will fix the user's connectivity problem.

Problems can occur with the network adapter driver. Unfortunately, the symptoms are never clear-cut, and often appear as intermittent connection problems, which can be a problem anywhere from the card itself to the cable, to the hub or router, or even with the server to which it's connected.

If you find that you are unable to connect to anything on the network, you need to focus more internally than elsewhere within the network. Reinstall the NIC drivers. After that, and depending upon how much acrobatics you really want to pursue, you probably want to check your cables across the board – make sure they're plugged into the computer properly, check the drop to the wall, check it from the wall (on the other side) to the hub, and check with other users to see if they're working okay. Now, things that you can do to help you with this: be prepared with at least one network cable that you know works well. Use it to replace and test the cable from the system to the wall. If there are no changes, replace everything, and use the same working cable to test between the wall (in the computer room, probably) to the hub. If there's no change there, try plugging the working cable into a functioning port. Check with your neighbors to ensure that the connections upstream from the port to other ports and out to the internet (if applicable) are working fine, and thus eliminating that much annoyance during the process. There are other things that you can do (cable and continuity testers, sniffers…) to test the network connection for a specific system, but these things definitely won't be on the exams, and the equipment in question is often in the hands of the phone technicians anyhow. Before you embark upon any of these tactics, it really is important that you determine if the problem is isolated or specific to a group of people. Knowing the layout of the cables in your building and in the hubs can save you some serious time by allowing you to determine if a hub has gone bad, or a specific upstream connection is in need of help. Again, these are definitely network-technician topics, which aren't exactly the primary focus of this book.

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.

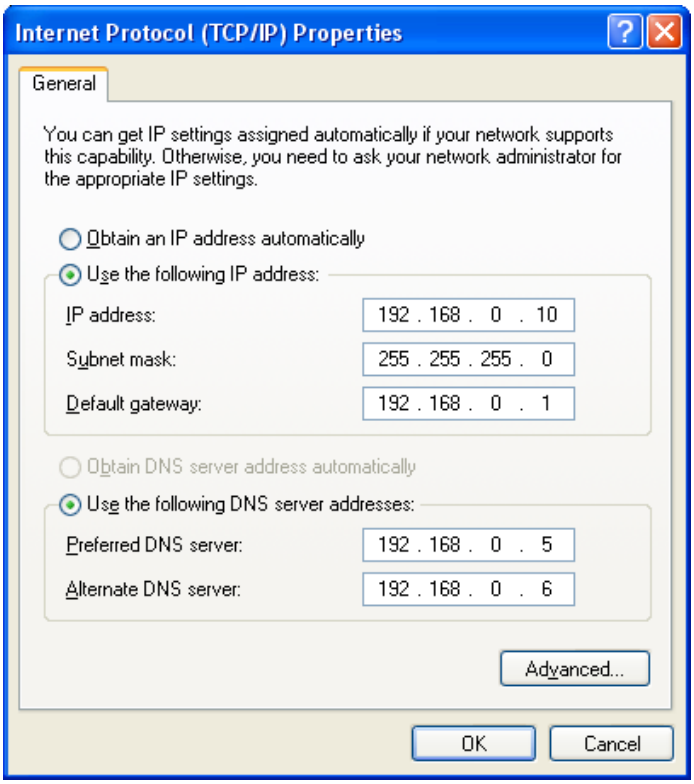

Figure: Configuring TCP/IP in Windows XP

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. Specify the IP parameters that should be used should the primary IP configuration fail.

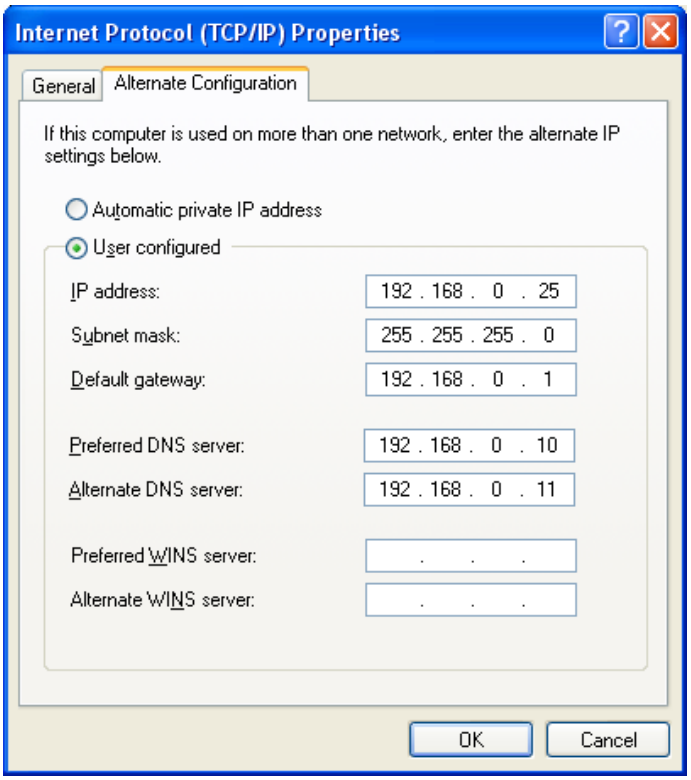

Figure: Windows XP Alternate Configuration

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 and update 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.

Most companies and home users now implement some sort of firewall solution to protect their networks. As a result, the Ping command is not as useful in troubleshooting as it used to be. This is because most firewalls block pings so you end up receiving false-positives. Due to such limitations, it is better to use application-layer programs to test connectivity. For example, running a Web browser will immediately indicate whether the computer has Internet connectivity.

Identify and troubleshoot network connectivity problems caused by the firewall configuration

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 accessible to attackers.

By implementing a firewall, you can close the door to your local computer and private network so intruders cannot get 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 network and requires little to no configuration. You can use it to secure a single computer with an Internet connection or to secure 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 an FTP 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 would not be 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 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.

You can make resources on the private network accessible to users on the Internet. For example, if there is a FTP server on the private network that you want to make available to Internet users. You can accomplish this by creating a static rule that will allow traffic on a specific port while still blocking traffic on all other ports.

One of the major limitations of ICF is that it is unable to filter outgoing traffic. If your network requires this functionality, you will have to implement a more advanced 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 ICF component of Windows XP can be enabled in a number of different ways. For example, you can enable it using the Network Setup Wizard. ICF can also be enabled manually using the Network Connection applet in the Control Panel.

You can use the following steps to enable the 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.

The Windows Firewall can run in client-only mode, which is also referred to as "On with no exceptions." This means that the firewall blocks all unsolicited inbound traffic without any reconfiguration by the user. You can configure the XP firewall to run in client-only mode by selecting the Don't Allow Exceptions option.

After you install service pack 2 for Windows XP you will see some unfamiliar utilities in the Control Panel. One of the new applets is called the Security Center and as the name implies, it's the place where you can manage the security settings on your computer.

Accessing this new feature is a cinch. Simply click Start, click Control Panel, and open the Security Center applet. The Security Center monitors the status of the three security essentials: Firewall, Automatic Updates, and Virus Protection. For example, if you disable the Windows Firewall component, it will indicate that the status is "OFF" and give you some recommendations that you should follow to increase security on your computer.

From the Security Center, you can also manage the security settings for Internet Options, Automatic Updates, and Windows Firewall. Clicking on any of these three links will bring up the appropriate dialog box. Along the side of the Windows Security Center dialog box, you will find a list of resources that you can use to stay on top of security.

Identify and troubleshoot problems with locally attached devices

Windows XP will include drivers for many different hardware components. In other cases, if your hardware is newer than service pack 2, drivers will not be available and Windows XP will not recognize it.

Most hardware will also come with a CD or floppy disk containing drivers. For optimal performance, it is generally recommended that you use the drivers included with the hardware or visit the manufacturers Web site and obtain the very latest driver. Some drivers may also be available through Microsoft Update. After installing Windows XP, you need to install the drivers for those hardware components that the Windows XP CD did not have drivers for. This might include drivers for the motherboard, video card drivers, sound card drivers, USB 2.0 drivers, and so on.

You may need to identify the make and model of the hardware component. This can be accomplished using Device Manager. Once you open the utility, you will see a list of all the devices that are currently installed.

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.

To open Device Manager:

1. Right-click My Computer and select Properties.
2. Select the Hardware tab.
3. Click the Device Manager button.

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 functionality:

- 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.

Most drivers come with specific installation instructions. You can also use Device Manager to install or update a driver.

1. From the Device Manager, double-click the type of device you want to update or change.
2. Click the Driver tab.
3. Click Update Driver to open the Hardware Update Wizard.
4. Accept the default option, Install the Software Automatically. Choose the Install from a List or Specific Location option if you have the updated driver so you can indicate the file location. Click Next.
5. Windows searches for an updated driver and instructs you if an updated driver has been found. Install the updated driver and click Finish.

If you have problems with hardware after upgrading the drive, you can use the device driver roll back function within Device Manager.

1. Within Device manager, 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.

Configuring Application Security

Identify and troubleshoot problems related to security permissions

Troubleshoot access to local resources

Local resources can be protected using NTFS permissions. In order to access resources stored on the local computer, the user account that you are logged on with must have the necessary permissions. If a user is unable to access a local resource or perform a specific task, it is more than likely a problem with NTFS permissions. For example, if a user attempts to delete a file on the local computer, but receives an access denied message, they do not have sufficient permissions.

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

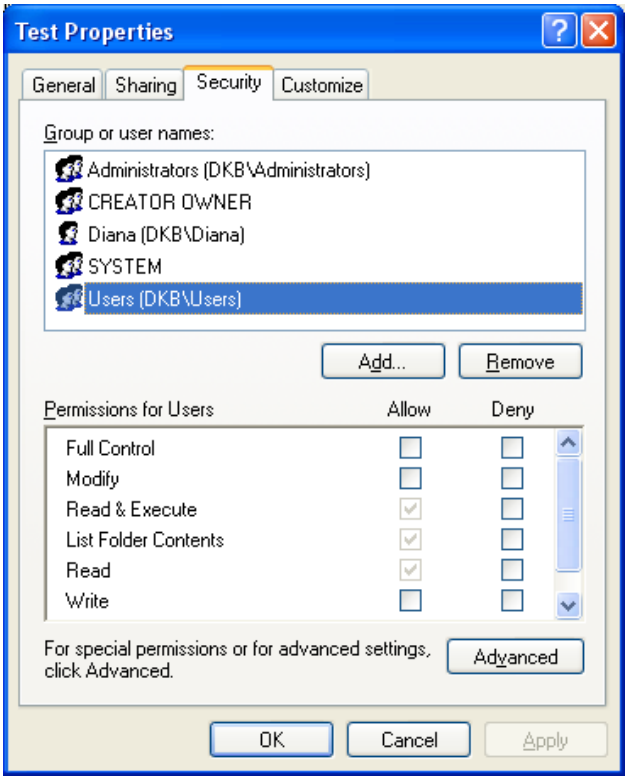

Figure: Standard NTFS permissions

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 the user 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. The user can also view the contents of subfolders.
- Read & Execute
  - The Read permission with 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 the Advanced button.

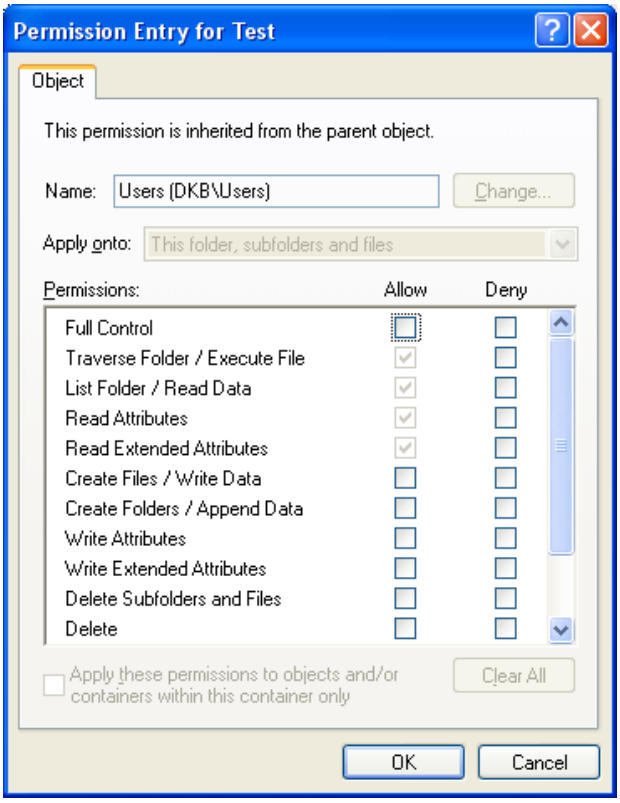

Figure: NTFS Special Permissions

You can assign NTFS permissions using the Security tab from a folder or file properties dialog box. By default, the Users group is assigned the Read, Read & Execute, and List folder contents permissions. A user can be assigned multiple NTFS permissions to a single resource. The effective permissions are cumulative. You can use the Effective Permissions tool to determine a user's or group's effective permissions for a specific resource.

Keep the following points in mind when troubleshooting NTFS permissions:

- NTFS permissions are cumulative.
- File permissions override folder permissions.
- Deny permission overrides all others.
- Simple file sharing must be disabled to set local permissions.
- Any user with Full Control over a resource can take ownership of it.

NTFS permissions can be affected when you copy or move a folder or file within or between NTFS partitions. This is important when it comes to troubleshooting access to local resources.

Most importantly, the only time a folder or file will retain its original permissions, is when it is moved within the same NTFS partition. Here is 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 also 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 permissions will once again be lost.

Troubleshoot access to network resources

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.

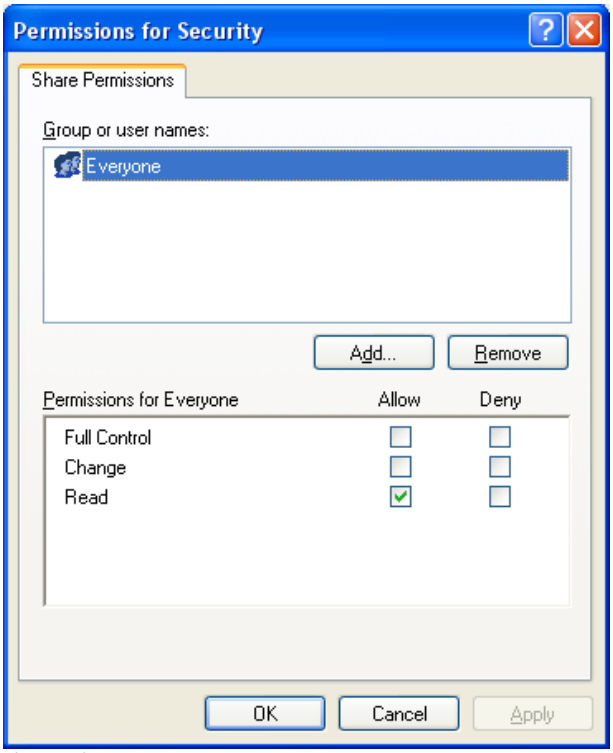

Figure: Share permissions

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.

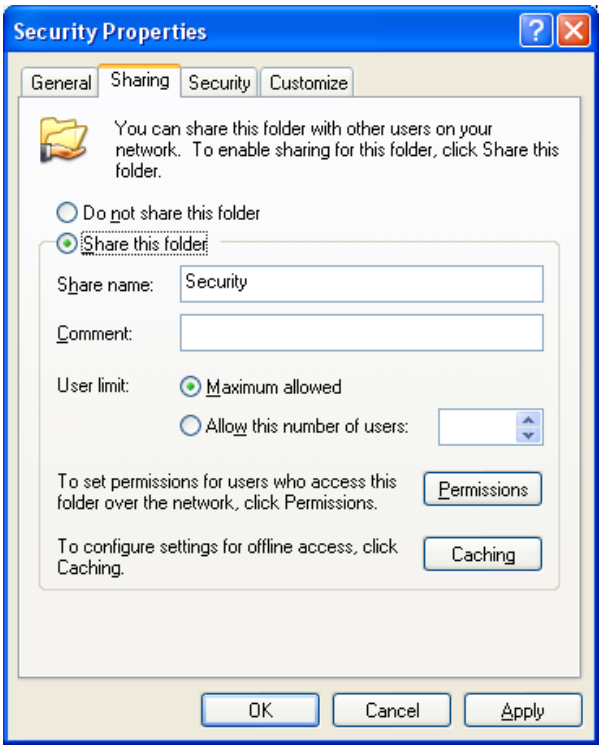

Figure: Creating a shared folder

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:

When a user accesses a resource from across the network, share permissions and NTFS permissions are combined. 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. This is important to remember when users are accessing network resources.

Troubleshoot insufficient user permissions and rights

The Effective Permissions tool is useful in troubleshooting permission problems. 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.

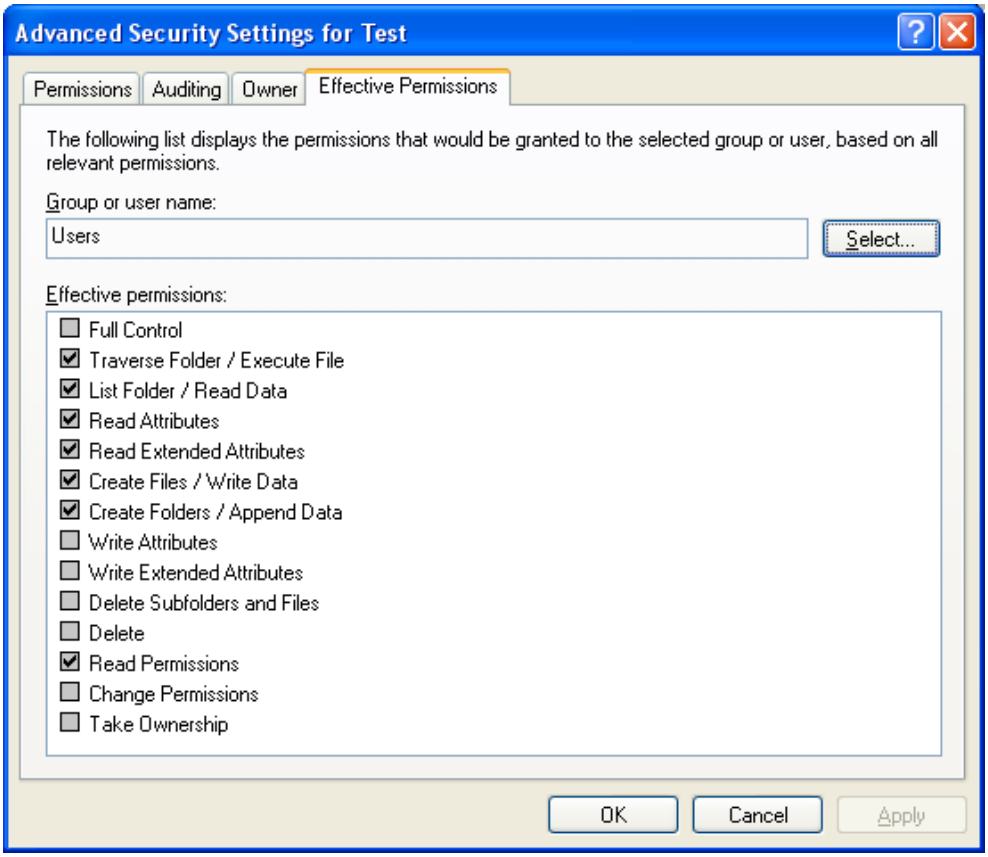

Figure: Identifying Effective Permissions

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 and the partition is formatted with NTFS, 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.
7. Restart the computer.

Figure: Enabling auditing in Windows XP

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

8. Open Windows Explorer.
9. Browse to the appropriate folder.
10. Right-click the folder and click Properties. Select the Security tab.
11. Click the Advanced button and select the Auditing tab.
12. Click the Add button to specify which users and groups you want to audit.
13. Type in the user or group name and click Check Names. Click OK.
14. Specify the type of events you want to audit by placing a check beside each one. Click Ok.
15. Click OK to close the Advanced Security Settings dialog box.
16. 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.

In order for users to perform certain tasks, such as backup and restore data, they must have the necessary user rights. Otherwise they will receive an error message. Rights can be assigned to users through the Local Security Policy using the User Rights Assignment container.

When you assign a user or group account a specific user right, you are entrusting that user to perform an administrative task. However, studies show that many of the threats and attacks against networks come from trusted users. With this in mind, you may want to set up auditing so you can monitor use of user rights.

Once you enable auditing of privilege use, an event will be written to the security log each time a user successfully or unsuccessfully attempts to exercise a user right. You can enable this feature by opening the local security policy (Control Panel | Administrative Tools | Local Security Policy). Expand the following containers: Computer Configuration | Windows Settings | Security Settings | Local Policies | Audit Policy. Double-click the option to Audit privilege use. Place a check beside Success and/or Failures (depending on the events you want to monitor). Click Ok. You can view any privilege use related events that occur by opening the Security log in the Event Viewer (Control Panel | Administrative Tools | Event Viewer).

Identify and respond to security incidents

Identify a virus attack

As a Desktop Support Technician, you have to be able to identify when a computer has been infected by a virus. Some of the behaviors you should be looking for include:

- Applications do not function properly.
- You cannot access your hard drive.
- New icons appear on the desktop.
- Unusual error messages appear.
- Unusual sounds unexpectedly come from your speakers.
- You experience a decrease in performance.
- Your computer has an unusually high level of disk drive activity.
- Data is missing.
- Your antivirus software is disabled and cannot be restarted.

One of the most important measures you can take to prevent viruses from infecting your computer is to install anti-virus software. Anti-virus software is a program designed specifically to detect and remove viruses, making it an essential application to install. Once you install anti-virus software, it will scan your computer and clean any viruses it finds. Some of the more popular anti-virus software programs are listed below.

- Trend Micro
- McAfee
- F-secure
- Symantec

- Computer Associates
- Panda Software

Most anti-virus software must be purchased or it may be included with the purchase of a new computer. Some vendors also offer specials or free trial periods. In any case, if you have just performed a clean installation of Windows, there will be no anti-virus software on your computer. The installation process will vary from vendor to vendor.

Since new viruses are constantly being created, the makers of anti-virus software have to constantly update their database with new fixes for detecting and removing them. So installing anti-virus software does not necessarily mean your system is secure. You have to make sure you update the signature files for the anti-virus software so it can detect and remove new viruses. Generally you can update the signature files over the Internet.

Signature files contain the latest virus updates. Therefore it's important to keep the signature files up-to-date. This can be done by downloading the latest files from the vendor's Web site. Not keeping the signature files up-to-date defeats the purpose of installing anti-virus software, as your computer will not be protected against the latest viruses.

Spyware is almost as undesirable as viruses because it can monitor your actions on the Internet and reduce your computer's performance. Some companies have been known to use spyware to gather data about customers. Even though it is not illegal, the spyware running on your computer may be tracking and sending data from your computer to another server on the Internet.

There is free software available on the Internet that you can download and use to scan your computer for unwanted software that may be tracking your movements. Microsoft has recently released its own product called Windows AntiSpyware.

As with installing anti-virus software, the steps for installing anti-spyware software will vary between vendors. You can normally find the installation steps on the vendors Web site.

Apply critical updates

To keep your system up-to-date, you can use Microsoft Update to detect outdated system files, find the latest security fixes and patches for your system, and any new enhancements. It is an easy way of keeping your system current with the latest product updates, and more stable over time.

With Automatic Updates, administrators can configure how and when Windows should be updated with the latest product updates. For example, updates can be downloaded automatically and installed at a preconfigured schedule.

The options available with Automatic Updates include:

- Notify Me Before Downloading Any Updates And Notify Me Again Before Installing Them On My Computer – Selecting this option means that before any updates are downloaded from the Microsoft Update site you will receive a notification. You will also receive notification before the updates are ready to be installed.
- Download The Updates Automatically And Notify Me When They Are Ready To Be Installed – Updates from the Microsoft Update site will be automatically downloaded. An icon will then appear with a message that the updates are ready to be installed. Clicking on the icon will launch the installation of the updates.

- Automatically Download The Updates And Install Them On The Schedule That I Specify – Any updates found on the Microsoft Update site will be downloaded in the background and installed at the pre-configured schedule.

You can configure Automatic Updates in Windows XP using the steps outlined below.

1. Open the Control Panel and switch to Classic View.
2. Double-click the System utility.
3. Click the Automatic Updates tab from within the System Properties window.
4. Select the option to Automatically download the updates, and install them on the schedule I specify.
5. Using the arrows beside the drop down box, select Every Sunday and select 12:00 am for the time.

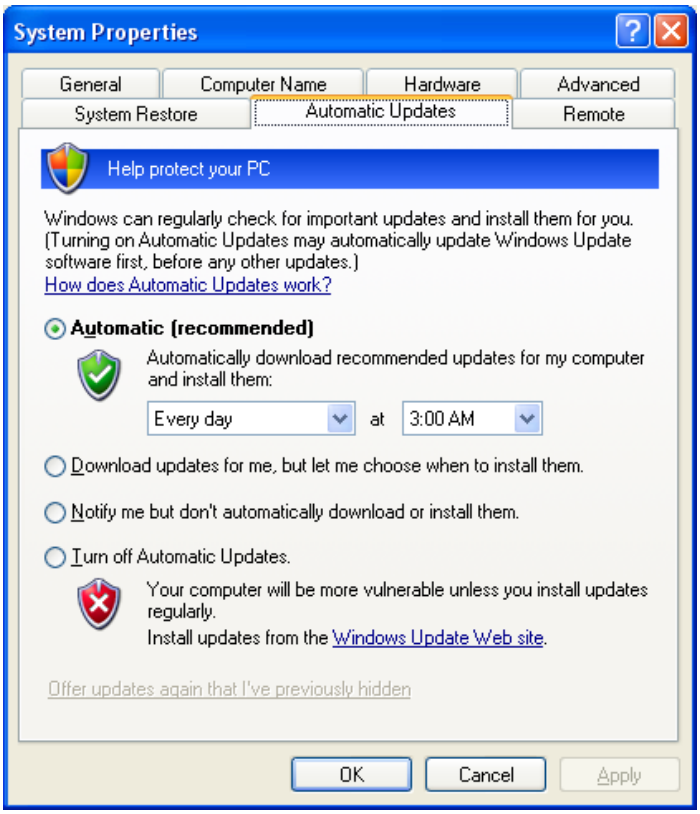

Figure: Configuring Automatic Updates settings

When updates (including service packs) are downloaded to your computer, a balloon will appear in the notification area indicating that your computer is ready to install them. Click the balloon and then click Express Install. Click Next to continue and select Restart Now if prompted.

You should proceed with more caution when it comes to installing a service pack. Installing service packs can result in additional problems because they include major changes and may add new features. You can follow these tips to minimize the problems that can occur from installing updates, hot fixes, patches, and service packs on your systems.

- Before you do anything, make sure you have performed a complete backup of your system.
- 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.
- If possible, perform the installation in a test environment first. This will give you a chance to see if there are any negative effects and how to remedy them.
- 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.
- 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.

SP2 for Windows XP can be obtained using a few different methods. The easiest way is to use Automatic Updates. Alternatively, you can download it from the Microsoft Update Web site or place an order for SP2 on a CD (you will have to wait for the CD to ship before installing it).

Manage application security settings

Outlook Express

Outlook Express can be configured to notify you before another application can send an email message without your knowledge. You can configure Outlook Express to do so using the Security tab from the Options dialog box and selecting the option Warn Me When Other Applications Try to Send Mail as Me. This option is enabled by default in Outlook Express 6.

Many users are often unable to differentiate between those attachments that are safe and those that are potentially harmful. Outlook Express can be configured to block attachments with certain extensions. You can do so by selecting the option Do Not Allow Attachments to Be Saved or Opened That Could Potentially Be a Virus.

With this option enabled, Outlook Express uses Internet Explorer's unsafe file list and the settings configured using the Folder Options applet to determine which attachments should be blocked. Typically, Internet Explorer considers any attachments containing script or code to be unsafe. You can configure which file types are unsafe by using the Folder Options applet within the Control Panel. When Outlook Express receives an email message with an attachment considered to be unsafe, a message appears notifying you that the attachment has been blocked.

Office Applications

Microsoft Office applications have various security features. You can access these features within any Office application using the Security tab from the Options dialog box shown in the figure below.

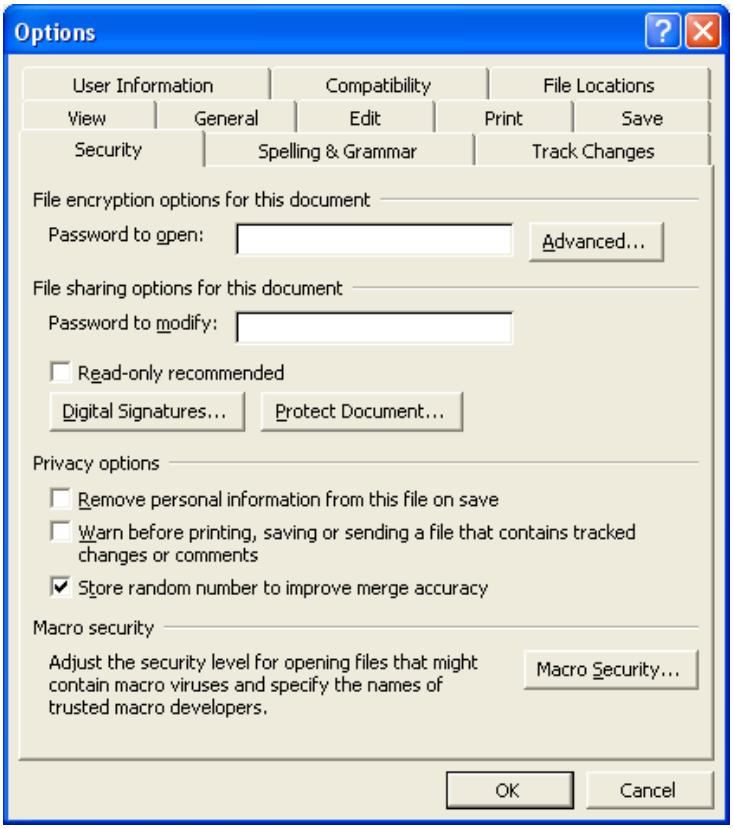

Figure: Microsoft Word security features

The security options available in Microsoft Outlook are described on the following table.

Options	Description
Secure Email	Allows a user to configure incoming and outgoing messages
Secure Content	Allows a user to set the security zone when viewing HTML messages
Digital IDs (Certificates)	Allows a user to get a new digital ID, import and export existing digital IDs, or publish existing digital IDs to the Global Address List (GAL)

Practice Questions

Chapter 1 Configuring and Troubleshooting Applications

1. You are a desktop support technician for a small company. All client computers are running Windows XP Professional with the latest service pack. The computers are members of the same workgroup.

   You have recently installed a custom application on all desktop computers. Users will use the new application to work with bitmap files.

   All users soon report that they have to open the bitmap files within the custom application. When they attempt to double click on a bitmap file, the Paint program opens instead. What should you do?

   Select the correct answer.

   - ❍ A. Change the file association for BMP files on each desktop.
   - ❍ B. Uninstall the custom application on each desktop. Deploy the applications through a group Policy object.
   - ❍ C. Uninstall the Paint program on each desktop.
   - ❍ D. Instruct users to use the Open With command for bitmap files and select the custom application.

2. You are the desktop support technician for Contoso Ltd. Client computers on the company network are running Microsoft Windows XP Professional. Several users work from home offices. These computers are running Microsoft Windows XP Home edition.

   A home user calls to report that Outlook Express does not launch when they open a saved email message. Instead, a third party email application that they recently installed opens. The user wants to use Outlook Express to open all saved messages. What should you instruct the user to do?

   Select the correct answer.

   - ❍ A. Open the Internet Options utility in the Control Panel. Use the Programs tab to configure Outlook Express as the default E-mail program.
   - ❍ B. Uninstall the third party E-mail application using the Add or Remove Programs utility in the Control Panel.
   - ❍ C. Instruct users to open the saved messages within Outlook Express.
   - ❍ D. Open the Folder Options utility in the Control Panel. Use the File Types tab to configure Outlook Express as the program used to open files with the DOC extension.

3. You are the desktop support technician for Contoso Ltd. Client computers are currently be upgrade from Windows 98 to Windows XP Professional.

   WRK10 is currently configured in a dual-boot configuration. Windows 98 is installed on C and Windows XP is installed on D. Volume C is formatted with FAT32 and volume D is formatted with NTFS. The computer also has two additional volumes:

   E: NTFS
   F: FAT32

   A custom application is installed on WRK10. It is accessible under both operating systems. User10 reports that they are unable to access files created with the application under Windows 98. The user can access the files under Windows XP. You discover that the files are being saved in the E:\Data\Custom directory.

   The user requires access to files under both platforms. What should you do?

   Select the correct answer.

   - ❍ A. Use the convert command and convert all NTFS volumes to FAT 32.
   - ❍ B. Assign the user Full Control permissions to the E:\Data\Custom directory.
   - ❍ C. Instruct the user to save all files to a directory on the F volume.
   - ❍ D. Open the Disk Management console and format volumes C and F with NTFS.

4. You are a desktop support technician for your company's Help Desk department. All client computers are running Microsoft Windows XP Professional and Microsoft Office 2003.

   A user calls to report that they have installed a new application on their home computer. He was logged on as administrator and placed a shortcut to the application on the desktop. However, when the user logs on with his account, the application is not available. What should you tell him to do?

   Select the best answer

   - ❍ A. Reinstall the application under his user account.
   - ❍ B. Add his user account to the Administrators group.
   - ❍ C. Instruct the user to log on as Administrator to run the application.
   - ❍ D. Copy the application's shortcut to the Desktop folder is his user profile.

5. You are a Desktop Support Technician for an Internet Service Provider. A customer calls you for assistance with setting up Outlook Express to connect to the ISP's mail servers.

   The customer wants to know what ports to specify for the incoming mail server and the outgoing mail server. What should you tell the customer?

   Select the best answer.

   - ❍ A. Use port 25 for incoming and outgoing mail.
   - ❍ B. Use port 25 for outgoing mail. Use port 110 for incoming mail.
   - ❍ C. Use port 110 for outgoing and incoming mail.
   - ❍ D. Use port 110 for outgoing mail. Use port 25 for incoming mail.

6. You are a Desktop Support Technician for your company's Help Desk department. A user calls to report a permission problem.

   The user has installed Windows 98 and Windows XP on their computer. Windows 98 is installed on C and Windows XP is installed on D. There are six additional computers in a workgroup.

   The user reports that all users were denied access to a file on D called Sales. However, when the file was moved to C, the file became accessible to other users. What should you tell the user?

   Select the best answer.

   - ❍ A. FAT does not support file level security.
   - ❍ B. Permissions are lost when moving between NTFS partitions.
   - ❍ C. The file permissions must be reconfigured after the file is moved.
   - ❍ D. Another user has taken ownership over the file and changed the permissions.

7. You are a Desktop Support Technician for your company. Client computers are running Windows XP Professional and Microsoft Office XP. The company network hosts its own Exchange server.

   A new employee calls to report that they can not read messages from home. The user can read his messages at the office. However, when he accesses his mailbox from his home computer during the evening, his messages are no longer in his mailbox. Any messages received during the say are no longer present. What is causing the problem?

   Select the best answer.

   - ❍ A. The SMTP server is not available to users during evening hours.
   - ❍ B. The POP3 server is not available during evening hours.
   - ❍ C. The user does not have permission to access their mailbox from home.
   - ❍ D. Outlook is not configured to leave a copy of read messages on the POP3 server.[TJN1]

8. You are a Desktop Support Technician for your company's help desk. Client computers are running Microsoft Windows XP Professional and Microsoft Office XP.

   The company recently hired a new user. The user calls to report that they are receiving a message that the computer is running low on disk space. You determine that the user has spent a lot of time on the Internet and using email. However, the user indicates that they have not been receiving messages with attachments. What is likely causing the problem?

   Select the best answer.

   - ❍ A. The History folder has reached the default value.
   - ❍ B. The user's personal folder file is too large.
   - ❍ C. The Temporary Internet Files folder has grown too large.
   - ❍ D. ActiveX controls have been installed on the computer.

9. You are a Desktop Support Technician for a small company. All computers are running Microsoft Windows XP Professional.

   A user calls to report that they want to make the company web page available even when they are not connected to the Internet. You determine that the user is currently using Internet Explorer to access the Internet. What should you instruct the user to do?

   Select the best answer.

   - ❍ A. Use the Favorites menu to add the web page as a favorite
   - ❍ B. Make the web page available offline when adding it as a favorite.
   - ❍ C. Save the web page onto your computer by selecting File, Save As.
   - ❍ D. Internet Explorer provides you with the option of making favorites available when you are offline.

10. You are a Desktop Support Technician for your company's help desk. Computers are running Microsoft Windows XP Professional. Microsoft Office 2003 has been deployed to all workstations.

    A user calls to report a problem when opening files with a .doc extension. Each time they double click a file with this extension, the file opens in Wordpad. The user wants the files to automatically open in Microsoft Word. What should you instruct the user to do?

    Select the best answer.

    - ❍ A. Open Folder Options applet and change the file association for files with the .doc extension.
    - ❍ B. Instruct the user to use the Open With command to open files with the .doc extension.
    - ❍ C. Instruct the user to open the files within Microsoft Word.
    - ❍ D. Uninstall Wordpad using the Add or Remove Programs applet.

Chapter 2 Resolving Issues Related to Usability

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

   A user calls to report that a new update has been released for Office XP's Word application. She wants to install the update but is unsure how to obtain it. What should you tell the user to do?

   Select the best answer.

   - ❍ A. Open Word and select Office on the Web from the Help menu.
   - ❍ B. Open Internet Explorer and navigate to the Windows Update Web site.
   - ❍ C. Open the System Properties window and enable Automatic Updates.
   - ❍ D. Select the Windows Catalog option from the Start Menu.

Chapter 3 Resolving Issues Related to Application Customization

1. You are a desktop support technician for your company. The network consists of 30 client computers all running Windows XP Professional and Microsoft Office 2003. Service pack 2 for Windows XP has been applied.

   All users store their Outlook data on the local computers. A user calls to report that they are unable to expand any of their folders in Outlook. You suspect that the user's Personal Folders file is corrupt.

   You need to recover the Outlook data. What should you do?

   Select the correct answer.

   - ❍ A. Within Outlook, launch the Detect and Repair option.
   - ❍ B. Locate and run scanpst.exe to repair the pst file.
   - ❍ C. Restore the user's Personal Folders File from backup.
   - ❍ D. Reinstall Microsoft Outlook using the Add or Remove Programs utility.

2. You are the desktop Support Technician for your company's help desk. All computers are running Windows XP Professional and Microsoft Office XP.

   You are configuring a computer for a new employee. You need to configure Internet Explorer's Temporary Internet Files folder settings to compromise between providing the best performance and up-to-date information when the employee is browsing Web sites that they have previously visited. Which option should you select?

   Select the best answer.

   - ❍ A. Every visit to the page.
   - ❍ B. Every time you start Internet Explorer
   - ❍ C. Automatically
   - ❍ D. Never

3. You are a Desktop Support Technician for a Help Desk Department. All computers on the network have been upgraded to Windows XP Professional. Users have administrative permissions to their own computers.

   A user reports that after making changes to the Internet Options settings, Internet Explorer is now slow when loading Web pages that the user has recently visited. The user wants Web pages displayed faster. What should you instruct the user to do to improve performance?

   Select the best answer.

   - ❍ A. Decrease the number of days Internet Explorer keeps pages in history.
   - ❍ B. Increase the amount of disk space for the Temporary Internet Files folder.
   - ❍ C. Move the Temporary Internet Folders file to another drive.
   - ❍ D. Configure Internet Explorer to check for updates to a Web page each time it is visited.

4. You are a Desktop Support Technician for your company's help desk. All computers on the nework have been upgraded to Windows XP Professional. Microsoft Office 2003 has also been installed.

   A user reports that each time they open a new Microsoft Word document, text from a document they created a week ago, appears in the new document. The user does not want this text to appear in any new documents they create. What should you instruct the user to do?

   Select the best answer.

   - ❍ A. Locate and delete the normal.dot template.
   - ❍ B. Delete the normal.doc template. Open a new Word document, delete the text, and save it as normal.doc.
   - ❍ C. Open the Normal.dot template, remove the unwanted text, and save it.
   - ❍ D. Use the Detect and Repair option from the Help menu in Word.

Chapter 4 Configuring and Troubleshooting Connectivity for Applications

1. You are a desktop support technician for Contoso Ltd. All client computers are running Microsoft Windows XP Professional with service pack 2 and Microsoft Office XP.

   A user has recently moved to a different department. His desktop computer was moved from one branch office to another. The user attempted to update his own IP address settings, however, the user now reports that they are no longer able to access the Internet.

   Upon investigation you discover that you can successfully ping computers on the local network and access local network resources. You can also access Web sites by IP address but not by name. What should you do to resolve the problem?

   Select the correct answer.

   - ❍ A. Run the ipconfig /flushdns command on the computer.
   - ❍ B. Change the IP address of the default gateway.
   - ❍ C. Configure the computer with the correct IP address for the DNS server.
   - ❍ D. Place an entry in the Hosts file for the Web servers that the user is attempting to access.

2. You are the Desktop Support Technician for a Windows Server 2003 network. All client computers are running Windows XP Professional. They are configured to use dynamic IP addressing.

   A user calls to inform you that they are unable to access any resources on the local network. You discover that the workstation is using the IP address of 169.254.2.10. No other users on the network are reporting any problems. What should you do?

   Select the best answer.

   - ❍ A. Run the Ipconfig command on the user's computer.
   - ❍ B. Ping the user's computer from your administrative computer.
   - ❍ C. Instruct the user to restart the computer.
   - ❍ D. Run the Ipconfig /renew command on the user's computer.

3. You are the Desktop Support Technician for a medium sized company that spans two buildings. Both buildings have subnets using DHCP servers. All client computers are running Windows XP Professional. They are configured to obtain an IP address from a DHCP server.

   One of the employees has moved to a new office in an adjacent building, taking his desktop computer with him. The user soon reports that they can no longer communicate on the network from within the new office. All other users in the office can access the network. What should you do?

   Select the best answer.

   - ❍ A. Ping the IP address of the DHCP server on the local subnet from the user's desktop.
   - ❍ B. Run the ipconfig /all command on the user's desktop.
   - ❍ C. Run the ipconfig /renew command on the user's desktop.
   - ❍ D. Configure the user's computer with a static IP address that is valid for the new subnet.

4. You are the Desktop Support Technician for your company's help desk. All client computers have recently been upgraded to Windows XP Professional. Microsoft Office 2003 has also been installed.

   A user reports that since the upgrade to Windows XP Professional, they are no longer able to open data DVD's using the computer's DVD drive. She requires access to this drive to view client information. What should you do?

   Select the best answer.

   - ❍ A. Check the vendor's Web site for an updated driver.
   - ❍ B. Use Device Manager to verify that the DVD drive is functioning correctly.
   - ❍ C. Use the Add Hardware Wizard to verify that there are no hardware conflicts.
   - ❍ D. Use the System Information to check that there are no IRQ conflicts.

5. You are configuring the IP parameters for the computers on the network. The network consists of multiple subnets. When specifying the IP parameters, each computer needs a unique IP address. What other parameters must you specify to so each computer can communicate on all networks?

   Choose all correct answers.

   - ❑ A. Subnet Mask.
   - ❑ B. IP address of a DHCP server.
   - ❑ C. IP address of the DNS server.
   - ❑ D. IP address of the default gateway.

6. You are the desktop support technician for a medium sized company. All computers are running Windows XP Professional.

   A user reports that they are trying to access the microsoft.com website but are unsuccessful. You determine that the user can access the site by its IP address but not its DNS name.

   What is causing the problem?

   - ❍ A. The gateway to the Internet is down
   - ❍ B. TCP/IP is incorrectly configured
   - ❍ C. There is an invalid DNS entry
   - ❍ D. The remote server is not online

Chapter 5 Configuring Application Security

1. You are a Desktop Support Technician for a small company. All client computers are running Microsoft Windows XP Professional and Microsoft Office XP.

   A user calls to report that their computer is behaving oddly. Everything seemed to be working yesterday. However, today the computer is running slow and several applications continuously hang. What should you tell the user to do?

   Select the best answer.

   - ❍ A. Scan the computer with anti-virus software.
   - ❍ B. Restart the computer.
   - ❍ C. Go to the Windows Update Web site and scan the computer for missing updates.
   - ❍ D. Reinstall the applications that are hanging.

2. You are a desktop support technician for your company. All computers are running Windows XP Professional and belong to a single workgroup.

   A user reports that they are concerned about the privacy of their data. They store a number of confidential documents on their computer. Permissions have been set to ensure only the appropriate users have access. The user would like to add another level of security to protect the data from theft in the event that the drive is stolen. What should you instruct the user to do?

   Select the best answer.

   - ❍ A. Back up the confidential files.
   - ❍ B. Encrypt the confidential files.
   - ❍ C. Compress the confidential files.
   - ❍ D. Rename the local Administrators account.

3. You are the desktop support technician for a workgroup. All computers are running Microsoft Windows XP Professional.

   You suspect that a user may be attempting to access a resource for which they are not authorized. The resource is a shared folder on one of the workgroups computers. You need to confirm your suspicions. What should you do?

   Select the best answer.

   - ❍ A. Verifying the permissions configured on resources.
   - ❍ B. Question the user you suspect is accessing the folder.
   - ❍ C. Using a network analyzer to capture network traffic.
   - ❍ D. Checking the security logs for any activity.

4. You are the desktop support technician for a help desk. All computers are running Windows XP Professional.

   A user on the network reports that a critical system file has been deleted. Upon questioning the user, you discover the problem started occurring after the user ran a program received through an email attachment. Several other users on the network who received the email are now reporting the same problem. What type of attack has occurred?

   Select the best answer

   - ❍ A. Virus
   - ❍ B. Social Engineering
   - ❍ C. Back Door
   - ❍ D. DoS Attack

Answers and Explanations

Chapter 1

1. Answer: A

Explanation A. By default, the Paint program is used to open bitmap images. You can change the file association for BMP files so the custom application is the default program used to open files of this type.

Explanation B. Uninstalling the application on each desktop is not necessary. How the application is deployed will not determine whether it is not default program used to open bitmap images.

Explanation C. Removing the Paint program on each desktop is not necessary. Users may still require access to it for opening files. It will also not ensure that the custom application is used to open bitmap files.

Explanation D. Although this solution would work, it would require users to use the Open With command each time they need to open a bitmap file. Changing the file associate is much easier for the end users.

2. Answer: A

Explanation A. Outlook Express can be configured as the default E-mail program through the Internet Options utility in the Control Panel.

Explanation B. It is not necessary to uninstall the third party e-mail application.

Explanation C. Although this solution would work, it is easier for end-users if you configure Outlook Express as the default E-mail program.

Explanation D. Saved e-mail messages will not have a DOC extension. This would result in all Word documents being opened with Outlook Express.

3. Answer: C

Explanation A. Windows 98 does not support NTFS volumes. By converting all volumes to NTFS, Windows 98 would no longer be accessible.

Explanation B. Assigning the user Full Control permission to the E:\Data\Custom directory would not resolve the problem. The volume is formatted with NTFS and Windows 98 does not support this file system.

Explanation C. The user should save all files to a directory on the F volume. Since this volume is formatted with FAT32, it is supported by both platforms. Any files saved to this volume will be accessible under both platforms.

Explanation D. You should not format volumes C and F with NTFS because Windows 98 does not support this file system.

4. Answer: D

Explanation A. It is not necessary to reinstall the application.

Explanation B. His user account should not be added to the Administrators group. The shortcut has been placed in the profile for the local Administrator account. Adding his user account to the Administrators group will not resolve the problem.

Explanation C. This does not provide an acceptable solution. Users should never be encouraged to log on with as the Administrator.

Explanation D. Once the shortcut is placed in his Desktop folder, it will be available to him when logging on with his user account.

5. Answer: B

Explanation A. Port 25 is used for sending email. However, it is not used for receiving email. The incoming mail server uses port 110.

Explanation B. Since port 25 is used for sending email, this port is specified for the outgoing mail server. Port 110 is used for receiving mail with POP3; therefore this port is specified for the incoming mail server.

Explanation C. Port 110 is used for receiving email. However, it is not used for sending email. The outgoing mail server uses port 25.

Explanation D. Port 110 is used for receiving mail. Port 25 is used for sending mail. With this configuration, the user will not be able to access the ISP's mail servers.

6. Answer: A

Explanation A. Windows 98 does not support NTFS; therefore you can conclude that this partition is formatted with FAT. FAT does not support file level security.

Explanation B. In this instance, the statement would be incorrect because partition C is not using NTFS. Windows 98 only supports FAT.

Explanation C. FAT does not support file level security. Permissions can only be set on folders.

Explanation D. FAT does not support ownership of folders and files. This is only a feature of NTFS.

7. Answer: D

Explanation A. An SMTP server is used for sending messages, not receiving.

Explanation B. If the POP3 server was unavailable, the user would not be able to access their mailbox during the evening. The user can access their mailbox; however, the messages received during the day are no longer available.

Explanation C. If this was the case, a message would appear indicating a permission problem.

Explanation D. If Outlook is not configured to leave a copy of messages on the Exchange server, they will only be available on the computer where they were received. Therefore, any new messages received on the user's office computer will be removed from the Exchange server and not be accessible from the home computer.

8. Answer: C

Explanation A. The History folder stores links to Web pages you have visited. By default it stores your history for the past 20 days. Since it just stores links, this folder does not use a large amount of disk space.

Explanation B. The user has not been receiving email attachments so their personal folder file should not be causing the problem.

Explanation C. The Temporary Internet Files folder is stored on C by default. This folder stores the Web pages you visit. The benefit is that it speeds up access to sites you have previously viewed. However, this folder can also consume a large amount of disk space.[TJN2]

Explanation D. ActiveX controls are used to enhance Web browsing. The are typically very small downloads so unlikely the cause of the problem.

9. Answer: B

Explanation A. Adding a web page as a favorite does not by default make it available to you when you are offline.

Explanation B. Adding a web page as a favorite does not make it available to you when you are offline. To make it available you must add the web page as a favorite and select the option to make available offline.

Explanation C. The Web page does not need to be saved.

Explanation D. Internet Explorer provides the option of making favorites available when not connected to the Internet.

10. Answer: A

Explanation A. If Wordpad is used to open files with a .doc extension, the file association has been changed. The file association can be changed from the Folder Options window.

Explanation B. This is not a suitable solution. The user files to automatically open in Microsoft Word.

Explanation C. This is not a suitable solution. It requires the user to launch Microsoft Word then open the files within this application.

Explanation D. It is not necessary to uninstall the applications. You need to tell Windows XP which program to use when opening specific file types. This is done through the file association.

Chapter 2

1. Answer: A

Explanation A. When a user selects Office on the Web from the Help menu, their Web browser will open to the Microsoft Office Online Web site. There will be a link on the Web site that will allow the user to check for new updates.

Explanation B. This Web site only contains updates pertaining to Windows XP and other versions of the operating system. It will not have updates for Microsoft Office.

Explanation C. Automatic Updates is used to keep the operating system up-to-date. It does not check for updates to Microsoft Office applications.

Explanation D. The Windows Catalog list provides information about hardware and software that is compatible with Windows XP.

Chapter 3

1. Answer: B

Explanation A. The Detect and Repair option is used to find and repair any errors with an office application. It is not used to repair Office data.

Explanation B. Scanpst.exe is used to repair a damaged Personal Folders (PST) file.

Explanation C. PST files are stored on local computers. The question does not indicate that there is a backup copy of the user's PST file.

Explanation D. It is not necessary to reinstall Microsoft Outlook. The application itself is not corrupt rather the data created and stored within the application is.

2. Answer: C

Explanation A. This option will decrease performance because a page is checked for updates each time the user visits it.

Explanation B. This option will decrease performance because a page is checked for updates each time Internet Explorer is restarted.

Explanation C. Internet Explorer will check for updates automatically. However, the frequency with which it does so depends on how often you visit a Web page.

Explanation D. Internet Explorer will never check the Web pages you have previously visited for updates.

3. Answer: B

Explanation A. This will determine how long links to recently visited Web pages are kept in the History folder.

Explanation B. Instruct the user to increase the amount of disk space for the Temporary Internet Files folder to improve performance.

Explanation C. This would improve performance if there was limited disk space. However, the question does not indicate that the problem is due to a lack of disk space.

Explanation D. This would decrease performance even more because Internet Explorer must check a Web page for updates each time it is visited before displaying it to the user.

4. Answer: C

Explanation A. The normal.dot template does not need to be deleted. The text in the template can be removed.

Explanation B. The Word template is called Normal.dot, not Normal.doc.

Explanation C. The Normal.dot template contains the settings applied to new Word documents. Open the template, delete the unwanted text, and save it. The text will no longer appear in Word documents.

Explanation D. This option should not be used. There is no problem with the installation of Word. The problem is that the Normal.dot template was mistakenly altered to include unwanted text.

Chapter 4

1. Answer: C

Explanation A. The user is unable to access any Internet resources. Therefore, emptying the contents of the cache will not likely resolve the problem.

Explanation B. Since you can access Web sites by IP address, the IP address of the default gateway is correct.

Explanation C. If the computer is moved, the IP address of the DNS server will have to be updated.

Explanation D. Although this solution will work, it would require more administrative effort than updating the IP address of the DNS server.

2. Answer: D

Explanation A. The ipconfig command displays the IP address, subnet mask, and default gateway assigned to a computer.

Explanation B. The ping command is used to test connectivity between two IP hosts. The computer is using Automatic Private IP Addressing when all other computers are obtaining IP addresses from the DHCP server. Therefore, the computer will not be able to respond to any ICMP messages sent to the computer using the ping command.

Explanation C. Restarting the computer may resolve the problem. However, the first step you should do is find out if the computer can obtain an IP address from the DHCP server.

Explanation D. This command is used to manually obtain an IP address from a DHCP server. The results of this would determine if the local computer is able to obtain an IP address from the DHCP server.

3. Answer: B

Explanation A. The user's computer is not able to communicate on the network. Therefore, pinging the IP address of the DHCP server would produce negative results.

Explanation B. This command will provide detailed information about the IP parameters on the local computer. The results will tell you what IP address is assigned to the computer allowing you to further troubleshoot the problem.

Explanation C. This command will force the computer to obtain an IP address from the DHCP server. However, you have not determined at this point what IP address the computer is using.

Explanation D. There is no need to configure a static IP address on the computer because the subnet uses a DHCP server. In doing so, there is also a chance of an IP address conflict occurring on the network.

4. Answer: B

Explanation A. Before installing an updated driver, you need to verify that the device is not functioning. This is done using Device Manager.

Explanation B. The first thing you should do is use Device Manager to verify that the device is functioning properly.

Explanation C. The Add Hardware Wizard is not used to check for hardware conflicts.

Explanation D. Before troubleshooting any hardware conflicts, you need to find out if the DVD drive is functioning or not. Device Manager will give you the status of the DVD drive.

5. Answers: A, C, D

Explanation A. In order for computers to communicate across all subnets on the network, you assign each computer a unique IP address, a subnet mask, and the IP address of the default gateway. The subnet mask is used to determine what subnet the computer is on. The default gateway allows computers to communicate outside their own subnet.

Explanation B. When configuring TCP/IP parameters on a computer you do not specify the IP address of the DHCP server. The IP address of the DNS server is optional.

Explanation C. No network can function without a DNS server.

Explanation D. In order for computers to communicate across all subnets on the network, you assign each computer a unique IP address, a subnet mask, and the IP address of the default gateway. The subnet mask is used to determine what subnet the computer is on. The default gateway allows computers to communicate outside their own subnet.

6. Answer: C

Explanation A. Since you can reach the remote computer by IP address your gateway is functioning.

Explanation B. Since you can access the Web server by IP address, TCP/IP is correctly configured.

Explanation C. If you are able to access a web server by IP address but not DNS name, there maybe an incorrect DNS entry in the zone file.

Explanation D. Since you can access the remote server by IP address, this would indicate that it is online.

Chapter 5

1. Answer: B

Explanation A. If a computer or the applications installed suddenly begin behaving oddly, the first thing you should do is scan the computer with anti-virus software.

Explanation B. Today, viruses are less of a threat because of technologies like Windows Firewall. I would recommend the following: Reboot the computer; Scan for updates from Windows Updates, and updates to the individual applications; Run anti-spyware software (much more common than viruses today); Run anti-virus software; Perform maintenance, such as cleaning up free space and defragging the disk.

Explanation C. It may be that some updates are missing. However, when a computer or application being behaving oddly for no reason, it is usually an indication that there is a virus.

Explanation D. It is not necessary to reinstall the applications. This type of solution should only be used as a last resort.

2. Answer: B

Explanation A. Files should always be backed up in the event of disaster but it does not protect them if the drive hosting the files is removed.

Explanation B. By encrypting the confidential files, any individual that attempts to open the files by removing the drive and placing it into another system will be unsuccessful.

Explanation C. Compressing files is done to increases available disk space.

Explanation D. Renaming the local administrators account will not prevent data from being read if the drive is removed. It is a good security practice though as it makes it more difficult for an individual to gain administrative access.

3. Answer: D

Explanation A. Verifying the permissions configured on resources is a good security practice but it will not tell you if someone has gained unauthorized access.

Explanation B. If a user is attempting to access a resource for which they are unauthorized they are unlikely to admit it.

Explanation C. A network analyzer will capture traffic but will not display the necessary information.

Explanation D. If auditing has been enabled you can check the security log. Any attempt by a user to access a resource for which they do not have permission will appear as an event within the log file.

4. Answer: A

Explanation A. One of the most common way for viruses to spread is through email attachments. Viruses are malicious programs that tell a computer to do something you do not want it to such as overwriting or deleting files.

Explanation B. A social engineering attack occurs when an individual attempts to gain access to a system to network by collecting classified information. One of the most common ways of gaining access to confidential information is by making phone calls to internal employees.

Explanation C. With a back door attack a program is installed that permits an unauthorized user access to a system.

Explanation D. A DoS attack attempts to reduce the quality of a service and make the service entirely unavailable.