



Microsoft 70-270

Installing, Configuring, and Administering Microsoft Windows
XP Professional

Q&A Demo

English: www.TestInside.com

BIG5: www.Testinside.net

GB: www.Testinside.cn

TestInside, help you pass any IT exam!

1. You are the desktop administrator for your company. A user reports that she is unable to use a new Bluetooth wireless headset with her Bluetooth-enabled Windows XP Professional computer.

You verify that the user's other Bluetooth devices work correctly. You discover that the user's computer is unable to detect the new headset. You follow the headset manufacturer's directions and ensure that the headset power is turned on correctly for normal operation.

You need to ensure that the user can use the new headset with her computer. What should you do?

- A. Put the headset in discovery mode.
- B. Put the user's computer in discovery mode.
- C. Join the computer to a Bluetooth Personal Area Network (PAN).
- D. Disable and then re-enable the Bluetooth software on the user's computer.

Answer: A

2. You are a desktop administrator for your company. A company user reports that he is unable to use his Bluetooth-enabled mobile phone with his Bluetooth-enabled Windows XP Professional computer. He is trying to play audio from the phone through the speakers on his computer.

You verify that other Bluetooth devices work properly with the user's computer. You test the speakers to make sure they are in working order. You also verify that the mobile phone can send output to a computer. You then discover that the phone cannot detect the computer.

You need to ensure that the user can use the phone with his computer. What should you do?

- A. Place the phone in Bluetooth discovery mode.
- B. Place the user's computer in Bluetooth discovery mode.
- C. Add the phone and the computer to the same Bluetooth Personal Area Network (PAN).
- D. Install mobile phone synchronization software on the user's computer.

Answer: B

3. You are a desktop administrator for your company. The company's software developers create a new application, which is packaged in an .msi file.

You are responsible for deploying this application to several users on the company network. Company policies require that applications be installed from a network location. They also require that application repair processes use the network location as the source for application files.

You need to prepare the application for deployment. What should you do first?

- A. Use the Msiexec.exe program to perform an administrative installation to a shared folder.
- B. Use the Msiexec.exe program to perform a passive installation to a shared folder.
- C. Copy the .msi file to a shared folder. Create a Group Policy object (GPO) that advertises the application to all users who will use the application. Point the GPO to the .msi file in the shared folder.
- D. Copy the .msi file to a shared folder. Create a logon script that executes the .msi file in unattended mode. Assign the logon script to all users who will use the application.

Answer: A

4. You are a desktop administrator for your company. You are responsible for deploying a new application. The application is packaged in an .msi file.

You need to deploy the application to only three users in the company. The .msi file contains all of the information necessary to correctly install the application.

You need to install the application so that users see information about the installation progress, but no other user interface is displayed during the installation. What should you do?

- A. Use the Msiexec.exe program to perform a quiet installation of the application.
- B. Use the Msiexec.exe program to perform a passive installation of the application.
- C. Create a Group Policy object (GPO) that assigns the application. Link the GPO to the site containing the users who will use the application.
- D. Create a Group Policy object (GPO) that advertises the application. Link the GPO to the domain.

Answer: B

5. You are a desktop administrator for your company. You need to deploy a new application. The application is packaged in an .msi file.

The application will be used by only a small number of users. You plan to install the application by using the Msiexec.exe program.

You need to ensure that the installation process does not display a user interface. What should you do?

- A. Manually perform a passive installation of the application.
- B. Manually perform a quiet installation of the application.
- C. Use a logon script to run the Msiexec.exe program.
- D. Use the Runas utility to run the Msiexec.exe program.

Answer: B

6. You are a desktop administrator for your company.

The company's software developers create an update for an existing line-of-business application. Only five users use this application. The update is packaged in a Windows Installer .msp file named Update.msp.

You need to install the update on the users' computers. What should you do?

- A. Install both the application and the update on your own computer. Create a Windows Installer transform (.mst file). Install the transform on the users' computers.
- B. Create a Group Policy object (GPO) that advertises the update. Link the GPO to the domain.
- C. On the users' computers, run the `Msiexec.exe /update update.msp` command.
- D. On the users' computers, run the `Msiexec.exe /I update.msp` command.

Answer: C

7. You are a help desk technician for your company.

Andrew is a salesperson who works remotely. Andrew uses a Windows XP Professional portable computer. He connects to the company network by dialing in to a company remote access server and logging on to the Active Directory domain. Andrew dials in to several different branch offices, depending on where he is located.

Andrew's user account is a member of the local Administrators group on his computer. He reports that he cannot enable Windows Firewall on a new dial-up connection that he created. In the past, he could enable Windows Firewall on dial-up connections that he created.

You need to ensure that Windows Firewall can be enabled on new dial-up connections that Andrew creates. What should you do?

- A. Remove Andrew's user account from the local Administrators group. Add his user account to the local Power Users group.
- B. Ask a domain administrator to remove the Prohibit use of Internet Connection Firewall on your DNS domain Group Policy setting on the domain. Instruct Andrew to connect to the company network and log on to the domain.
- C. Instruct Andrew to disable Internet Connection Sharing (ICS) Discovery and Control on his computer. Instruct Andrew to delete and then re-create the new dial-up connection.
- D. Instruct Andrew to delete and then re-create the new dial-up connection. Instruct Andrew to share the new dial-up connection by using Internet Connection Sharing (ICS).

Answer: B

8. You are the network administrator for your company. All employees use Windows XP Professional computers. Many employees work from home and connect to the company network by using PPTP virtual private network (VPN) connections.

An employee named Andrea reports that she cannot connect to the network over her new DSL connection. You confirm that the connection is configured correctly in Network Connections. However, when Andrea attempts to establish a connection to the VPN server vpn1.contoso.com, she receives the following error message. "Unable to establish the VPN connection. The VPN server may be unreachable or the security parameters may not be configured properly for this connection."

No other employees who use cable modem or DSL connections report similar problems. You verify that Andrea's DSL provider permits VPN traffic on its network.

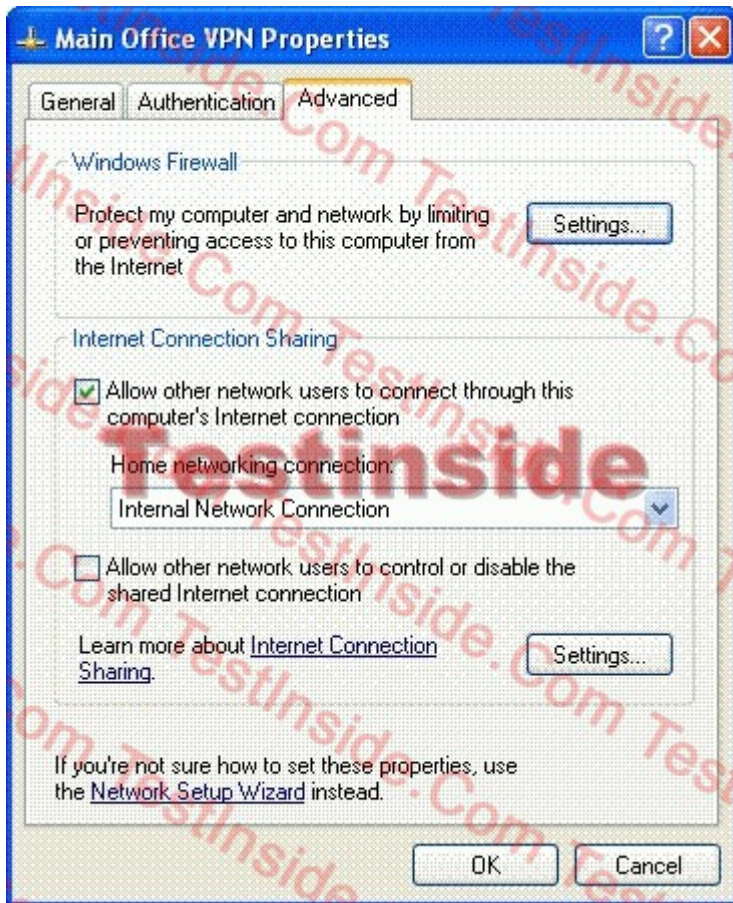
Andrea needs to be able to establish a connection to the company network. What should you do?

- A. Configure Andrea's DSL modem to allow TCP port 1723 and IP protocol 47 to pass through the connection.
- B. Configure Windows Firewall on Andrea's computer to allow incoming VPN connections.
- C. Configure the VPN connection to use the IP address of the VPN server rather than the host name of the VPN server.
- D. Configure the TCP/IP properties of the VPN connection to include the IP address of a DNS server on the company network.

Answer: A

9. You are the network administrator for one of your company's branch offices. Ten employees work in the branch office. All client computers in the branch office run Windows XP Professional. All client computers have manually configured IP addresses in the 192.168.1.0/24 range.

The branch office has a cable modem connection to the Internet. All employees in the branch office need access to the main office by means of a virtual private network (VPN) connection over the Internet. The VPN connection is configured as shown in the exhibit. (Click the Exhibit button.)



Employees in the branch office report that they cannot access resources that are located on the main office network. You investigate and discover that you can establish a VPN connection locally on a client computer named Pro1 and can access main office network resources. However, you cannot connect to Pro1 from other computers on the branch office network.

You want all employees in the branch office to be able to access main office network resources by means of the VPN connection on Pro1. What should you do?

- A. Disable Windows Firewall on the main office VPN connection.
- B. Add a port exception to Windows Firewall to allow incoming PPTP traffic on the main office VPN connection.
- C. Select the Allow other network users to control or disable the shared Internet connection check box.
- D. Configure all client computers in the branch office to obtain IP addresses automatically.

Answer: D

10. You are a desktop administrator for your company.

A user reports that whenever she visits certain Internet Web sites, additional Web browser windows open automatically. The user's computer runs Windows XP Professional with Service Pack 2 (SP2). She uses Microsoft Internet Explorer as her only browser.

You need to prevent additional windows from opening automatically when the user visits a Web site. You want to accomplish this as quickly as possible and with the minimum number of changes to the user's computer.

What should you do?

- A. Configure Internet Explorer to reject cookies from Web sites.
- B. Configure Internet Explorer to block pop-up windows.
- C. Configure Windows Firewall to block inbound traffic from TCP port 80.
- D. Configure Windows Security Center to not display antivirus and firewall warnings.

Answer: B

11. You are a desktop administrator for your company. The company network includes an Active Directory domain. All client computers are members of the domain.

A user reports that he cannot connect to his Windows XP Professional computer by using Remote Desktop. You verify that the computer is running Windows XP with Service Pack 2 (SP2) and that Remote Desktop is enabled.

You attempt to configure Windows Firewall to allow the Remote Desktop Protocol (RDP), but you discover that the configuration dialog box is unavailable (appears dimmed).

You need to ensure that the user can use Remote Desktop to connect to his computer. Your solution must involve the minimum number of changes to the computer's configuration.

What should you do?

- A. Configure Windows Security Center to display firewall warnings.
- B. Install a third-party hardware firewall and disable Windows Firewall.
- C. Set up domain Group Policy objects (GPOs) so that the GPO that enforces the No exceptions Windows Firewall policy does not apply to this user's computer.
- D. Create and link a Group Policy object (GPO) that disables Windows Firewall on the user's computer.

Answer: C

12. You are a help desk technician for your company. The company network consists of a single Active Directory domain. All client computers run Windows XP Professional.

The help desk technicians use Remote Assistance to remotely control user sessions to provide online support to users. The users currently use Microsoft Exchange and Microsoft Outlook to submit Remote Assistance invitations to the help desk technicians.

Stephen is a user in the sales department. Stephen has a portable computer and frequently travels to customer

locations. While Stephen is in the corporate office, he submits a Remote Assistance invitation to the help desk. When you attempt to answer the invitation and establish the Remote Assistance session, you receive the following error message.



You verify that Stephen's computer is connected to the network and that he did not cancel the invitation. You also verify that the invitation did not expire. You do not experience similar problems when establishing Remote Assistance sessions with other computers.

You need to be able to establish a Remote Assistance session with Stephen's computer. What should you do?

- A. Enable the Remote Assistance program exception in Windows Firewall on Stephen's computer.
- B. Add your user account to the Remote Desktop Users group on Stephen's computer.
- C. In the System properties for Stephen's computer, select the Allow users to connect remotely to this computer option, and add your user account to the list of allowed users.
- D. In the local security policy for Stephen's computer, grant your user account the Allow logon through Terminal Services user right.

Answer: A

13. You are a help desk technician for your company. Your Windows XP Professional computer is connected to the company network, which is connected to the Internet via a T1 line. Your computer hosts a Web site that is accessed by other help desk technicians.

You set up a new Windows XP Professional computer at home. The home computer is connected to the Internet via a cable modem that is always on. The home computer is configured to use a static IP address assigned by your Internet Service Provider (ISP).

You want to use Remote Desktop Connection to control your home computer while you are at work. However, you want to prevent any other incoming Internet traffic from reaching the home computer. You verify that your company's Internet firewall permits Remote Desktop Connection traffic.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two.)

- A. On your office computer, enable Windows Firewall.

- B. On your office computer, enable Internet Connection Sharing (ICS).
- C. On your home computer, enable Internet Connection Sharing (ICS).
- D. On your home computer, enable Windows Firewall.
- E. On your home computer, enable the Remote Desktop program exception in Windows Firewall, and clear (disable) all other program exceptions.
- F. On your home computer, enable the Remote Assistance program exception in Windows Firewall, and clear (disable) all other program exceptions.

Answer: D AND E

14. You are the desktop administrator for your company. You set up a new Windows XP Professional computer at home. The computer is always connected to the Internet via an ADSL modem.

You enable Windows Firewall on the ADSL connection. After several days, you notice that the computer is running slower than normal.

You examine the Windows Firewall log file. A portion of the log file is shown here.

```
2001-10-25 15:28:36 CLOSE TCP 172.30.23.1 172.30.23.103 3738 80 - - - - -  
2001-10-25 15:28:36 CLOSE TCP 172.30.23.104 172.30.23.103 1076 80 - - - - -  
2001-10-25 15:28:53 OPEN-INBOUND TCP 172.30.23.104 172.30.23.103 1077 80 - - - - -
```

You want to prevent the activity shown in the log. How should you configure Windows Firewall?

- A. Disallow the exception for Telnet traffic.
- B. Disallow incoming Internet Control Message Protocol (ICMP) echo requests.
- C. Disallow the exception for HTTP traffic.
- D. Disable the logging of successful connections.

Answer: C

15. You are a help desk technician for your company. Stefan and Irene are software developers for the company. Stefan is developing a Web application on his Windows XP Professional computer. The computer is named Stefan132. All client computers use Microsoft Internet Explorer 6.0 or later as their Web browser.

When Irene types `http://Stefan132` in the Address bar of her Web browser, she cannot access the Web application. However, Stefan can access the Web application by typing `http://localhost` or `http://Stefan132` in the Address bar of his Web browser. He can also access resources on the company network.

When you run the Ping command on your computer, you cannot connect to Stefan's computer. When you attempt

to access <http://Stefan132> from your computer, Internet Explorer displays “DNS or Server Error.”

You need to ensure that Irene can access the Web application on Stefan’s computer. First, you establish a Remote Assistance connection to Stefan’s computer.

What should you do next on Stefan’s computer?

- A. Run the `IPconfig /renew` command.
- B. Stop and then restart the World Wide Web Publishing service.
- C. Ensure that the Everyone group has Allow - Full Control permission on the Inetpub folder.
- D. In the properties of the Local Area Connection connection, allow a Windows Firewall exception for port 80.

Answer: D

16. You are the administrator of a Windows XP Professional computer named Pro1. The computer is connected to the Internet. Pro1 provides Internet access to five other Windows XP Professional computers that are connected to Pro1.

You enable Internet Connection Sharing (ICS) and Windows Firewall on Pro1.

Users on the five computers can successfully ping Pro1. The Pro1 computer can successfully ping Internet sites. However, users on the Internet do not receive a response when they use the Ping command to test the connection to Pro1.

You want to ensure that users on the Internet can successfully use the Ping command to test the connection to Pro1.

What should you do?

- A. Configure the connection to the Internet to bridge the connection.
- B. Change the TCP/IP settings on Pro1 to enable TCP/IP filtering.
- C. Configure Windows Firewall to enable Internet Control Message Protocol (ICMP) echo requests.
- D. Add a new service exception named Ping to Windows Firewall. Use external port number 8 and internal port number 8 for this service exception.

Answer: C

17. You are the administrator of a Windows XP Professional computer named Pro1. The computer is connected to the Internet. Pro1 provides Internet access to eight other Windows XP Professional computers that are connected to Pro1.

You enable Internet Connection Sharing (ICS) and Windows Firewall on Pro1.

You run an application named App1 on Pro1. App1 communicates with an online training company on the Internet.

To display an online seminar, the training company needs to contact the App1 application at port 5800.

You want to ensure that the training company can connect to the App1 application. What should you do?

- A. Configure Windows Firewall to enable the Internet Control Message Protocol (ICMP) Allow redirect option. Then start the App1 application that opens port 5800.
- B. Create a new service exception named App1. Use port 5800 as both the external and internal port number.
- C. Edit the %systemroot%\System32\Drivers\Etc\Services file on Pro1 to include a service definition named App1 for port 5800.
- D. Change the TCP/IP settings on Pro1 to enable TCP/IP filtering. Permit network traffic on port 5800.

Answer: B

18. You are the administrator of all the Windows XP Professional portable computers in your company. All these computers are members of a Windows 2000 domain.

During the day in the office, users connect their portable computers to the company network. In the evening at home, users use their portable computers to access the Internet.

Users report that when they connect their portable computers to the company network, they are able to access network resources. However, users on the network are not able to connect to shared folders that are defined on the portable computers. You verify that the users have the necessary permissions to connect to the shared folders on the portable computers.

You want to ensure that the portable computers are protected when they are connected to the Internet in the evening. You also want to ensure that users can access shared folders on the portable computers during the day.

What should you do?

- A. On the Windows XP Professional portable computers, enable Internet Connection Sharing (ICS) Discovery and Control.
- B. Configure the network TCP/IP settings on the Windows XP Professional portable computers to use DHCP. Configure the Alternate Configuration feature to use user-configured addresses.
- C. Link a Group Policy object (GPO) to the company network sites. Configure the GPO to enable Guest only sharing and security model for local accounts.
- D. On the Windows XP Professional portable computers, enable Windows Firewall. Configure the local Group Policy object (GPO) to enable Prohibit the use of ICF on your DNS domain network.
- E. On the Windows XP Professional portable computers, enable Windows Firewall. Configure the local Group Policy object (GPO) to enable Prohibit Enabling/Disabling components of a LAN connection.

Answer: D

19. You are the network administrator for your company. The network includes an Active Directory domain. All client computers are members of the domain.

A Windows XP Professional computer named Client1 runs a line-of-business application that is used by several users. These users log on to Client1 by using local user accounts. These accounts have been granted the specific permissions that are necessary for the application to function. Users do not use local accounts on other client computers.

Domain users currently change their passwords every 45 days. You need to ensure that the users of Client1 change their local account passwords every 20 days.

What should you do?

- A. Configure local security policy on Client1 so that it has a maximum password age of 20.
- B. Configure the Default Domain policy in the domain so that it has a maximum password age of 20.
- C. Configure local security policy on Client1 so that it has a password history of 20.
- D. Configure the Default Domain policy in the domain so that it has a password history of 20.

Answer: A

20. You are a network administrator for your company. The network includes a single Active Directory domain. All client computers are members of the domain.

A Windows XP Professional computer named Client1 is used by the human resources (HR) department. This computer contains sensitive information that must be available only to department employees.

A human resources employee reports that another network administrator accessed Client1. You discover that the network administrator used his domain administrative account to log on to Client1 with administrative privileges.

You need to ensure that domain administrators cannot log on to Client1 with administrative privileges. What should you do?

- A. Join Client1 to a workgroup named HR.
- B. Modify the user rights on Client1 so that members of the Domain Admins group do not have the Log on interactively user right.
- C. Remove the Domain Admins group from the local Administrators group on Client1.
- D. Add the Authenticated Users group to the local Administrators group on Client1.

Answer: C