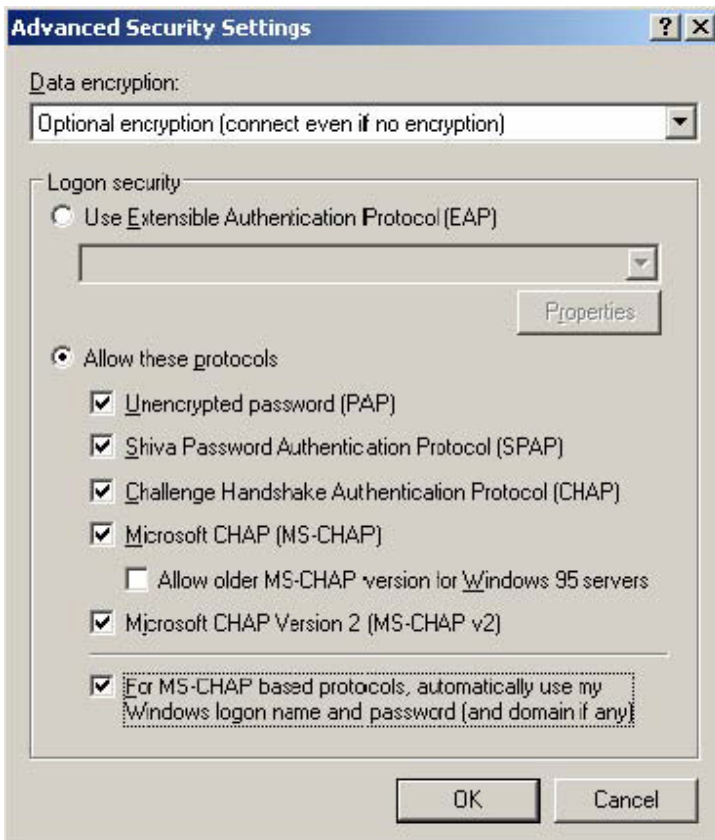


QUESTION 201

You are creating a dial-up connection on your Windows 2000 portable computer to connect to your customer's dial-up server. You are not sure which type of server your customer is using for dial-up connections. You want to ensure that your dial-up connection authentication is secure and that your logon information is not sent in plain text. You view the Advanced Security Settings dialog box as shown in the exhibit.



Which option or options should you disable in the Advanced Security Settings dialog box? (Choose all that apply)

- A. Unencrypted password (PAP)
- B. Shiva Password Authentication Protocol (SPAP)
- C. Challenge Handshake Authentication Protocol (CHAP)
- D. Microsoft CHAP (MS-CHAP)
- E. Microsoft CHAP Version 2 (MS-CHAP v2)
- F. For Microsoft CHAP based protocols.

Answer: A

Explanation: PAP is the least complicated authentication protocol and sends passwords in plain text.

070-210

Passwords are thus not encrypted passwords. This authentication protocol is used when a more secure means of authentication cannot be negotiated between two computers. You should therefore disable PAP to ensure that login information is not sent in plain text.

Incorrect answers:

B: SPAP does not support data encryption. Instead it uses a reversible encryption authentication mechanism.

C: CHAP was designed to overcome the problem of sending passwords in plain text and encrypts the authentication process by using a challenge-response method of authentication known as Message Digest 5.

D: MS-CHAP is an improvement of CHAP and uses a similar challenge-response method of authentication.

E: MS-CHAP v2 provides more advanced and improved features than CHAP and MS-CHAP. It uses mutual authentication, stronger data encryption keys and different encryption keys for sending and receiving data.

F: All CHAP protocols use an encryption mechanism in the authentication process.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 1

QUESTION 202

You want to connect to your company network from your Windows 2000 Professional computer at home. You have an ISDN line that is used for Internet connectivity. You create a VPN connection and are able to connect successfully to the company network. While connected to the company network, you are unable to access the Internet.

What must you do so that you can access the Internet?

- A. Configure the ISDN connection to use SLIP instead of PPP.
- B. Select the Enable Internet Connection Sharing for this connection check box in the ISDN connection properties.
- C. Clear the Use default gateway on remote network checkbox.
- D. Install and configure the SAP Agent service.

Answer: C

Explanation: If the connection is using the default gateway on the remote network, it will be able to access computers on the remote network but it will not be able to access Internet.

Incorrect answers:

A: SLIP is a legacy protocol. It can only be used on servers. It enables a remote connection from a Windows 2000 Server to a UNIX server, which cannot handle PPP.

B: Internet Connection Sharing would enable the sharing of this connection at the client side. It will not help to solve the problem of Internet connectivity.

C: SAP is a distance-vector-based advertising protocol commonly used on IPX internetworks to advertise

services and their locations. RRAS also provides the ability to configure static SAP services and SAP service filters. SAP service filters reduce unneeded SAP traffic from being sent to the RRAS connection. Installing and configuring a SAP Agent service is thus not appropriate to this scenario.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 2

QUESTION 203

You want to configure your Windows 2000 Professional computer to remotely access your company's Windows 2000 Routing and Remote Access server. You configure a VPN connection. For security purposes, you configure the VPN connection to use MS-CHAP v2 only and to require encryption. You also configure TCP/IP to obtain an IP address automatically, to enable IPsec, and to set IPsec to Secure Server.

When you try to connect, you receive the following error message, "The encryption attempt failed because no valid certificate was found."

What should you do to connect to the server?

- A. Enable the VPN connection to use MS-CHAP.
- B. Change the data encryption setting to Optional Encryption.
- C. Specify a TCP/IP address in the Network properties.
- D. Change the IPsec policy setting to Client.

Answer: D

Explanation: In this scenario the client and the server are able to make some initial communication but then the encryption negotiation failed. The Server is configured to use the Secure Server (Require Security) policy, which does not allow unsecured communications with clients. By changing the policy at the server to Client (Respond Only) policy, plaintext communications would be allowed. The Client (Respond Only) policy effectively allows clear-text communication but will attempt to negotiate security if a security request is made.

Incorrect answers:

A: Since both the client and the Server are Windows computers there is no need for MS-CHAP. MS-CHAP is sometimes used on downlevel Windows clients, for example Windows 98, which does not support MS-CHAP v2 by default.

B: Even if the data encryption setting on the client is set to Optional Encryption the RRAS server will still use the Secure Server setting, which will not accept unencrypted traffic. Therefore this option does not provide a solution for this problem.

C: The client and the server were able to communicate, although there is a disagreement on encryption. Therefore an IP address has been leased and there is thus no need to specify a TCP/IP address in the Network properties.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part

IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 2

QUESTION 204

You use a Windows 2000 Professional computer at home. You need to access shared files on a server named server1. This server is on your company's network and is not accessible from the Internet. Your company's network also includes a third party VPN server that is accessible from the Internet. You dial in to your Internet service provider and then create a VPN connection to your company's VPN server. After the connection is successfully established, you run the net view \\server1 command and receive the following error 'the server is inaccessible or could not be found'.

You need to access the shared files on server 1. What should you do?

- A. Stop and then start the TCP/IP NetBIOS helper service on your computer.
- B. Stop and then start the DNS client service on your computer.
- C. Add a HOSTS entry for server1 to your computer.
- D. Add a LMHOSTS entry for server1 to your computer.

Answer: D

Explanation: By adding a LMHOST entry for server1, the home computer will be able to access the Server by using its NetBIOS name.

Incorrect answers:

A: Stopping and starting the TCP/IP NetBIOS service will not solve the problem in this scenario.

B: The name Server1 is a NetBIOS name, not a DNS name. Therefore, stopping and then restarting the DNS client service will not solve the problem in this scenario.

C: HOST files map DNS entries, but Server1 is not a DNS name, it is a NetBIOS name. Therefore you do not require HOST entries for Server1 on our computer.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 2

QUESTION 205

You are the network administrator for Certkiller .

You need to connect to Certkiller 's network from your Windows 2000 Professional computer at home. You have a DSL line that is used for Internet connectivity. You create an L2TP virtual private network (VPN) connection and are able to connect successfully to Certkiller 's network. While connected to Certkiller 's network, you are unable to access the Internet.

You want to be able to access the Internet while connected to Certkiller 's network.

How should you configure the connection properties?

070-210

- A. Configure the DSL connection to use PPTP instead of L2TP.
- B. Enable Internet Connection Sharing for the DSL connection properties.
- C. Clear the Use default gateway on remote network check box.
- D. Clear the Require data encryption check box.

Answer: C

Explanation: When you connect to the internet with a DSL connection, your default gateway will be the address of the ISP's router. This enables you to connect to the internet. When you create a VPN connection to a Routing and Remote Access server, the default settings will change your default gateway to that of the remote network. This means that you won't be able to connect to the internet via your ISP. To be able to access the Internet while connected to the remote network, you need to clear the Use default gateway on remote network check box.

Incorrect Answers:

A: You are able to successfully connect to the remote office using L2TP. Therefore, you don't need to connect using PPTP.

B: You don't want to share your internet connection so you don't need to enable Internet Connection Sharing.

D: You are able to successfully connect to the remote office, so your encryption settings must be correct.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 2

QUESTION 206

You are the network administrator for Certkiller .

You configure an L2TP virtual private network (VPN) connection on your Windows 2000 Professional computer to remotely access Certkiller 's Windows 2000 Routing and Remote Access server. The server is configured to accept a limited number of both PPTP and L2TP connections. You configure the VPN connection to use MS-CHAP v2 only and to require encryption. You also configure TCP/IP to obtain an IP address automatically. Many times when you try to connect, you are unable to because all of the ports are in use. Other times you are able to connect successfully.

You want to increase your chances of being able to connect to the server while ensuring that the most secure connection type available is used.

What should you do?

- A. Enable the VPN connection to use MS-CHAP.
- B. Specify a TCP/IP address in the Network properties.
- C. Change the data encryption setting to Optional Encryption.
- D. Configure the Type of VPN server I am calling to be Automatic.
- E. Configure the Type of VPN server I am calling to be PPTP.

Answer: E

Explanation: PPTP assumes the availability of an IP internetwork between a PPTP client (a VPN client using the PPTP tunneling protocol) and a PPTP server (a VPN server using the PPTP tunneling protocol). The PPTP client might already be attached to an IP internetwork that can reach the PPTP server, or the PPTP client might have to dial into a network access server (NAS) to establish IP connectivity as in the case of dial-up Internet users. Authentication that occurs during the creation of a PPTP-based VPN connection uses the same authentication mechanisms as PPP connections, such as Extensible Authentication Protocol (EAP), Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP), CHAP, Shiva Password Authentication Protocol (SPAP), and Password Authentication Protocol (PAP).

The server is configured to accept a limited number of PPTP and L2TP connections, thus if you want to increase your chances to connect to the server with the most secure connection type available under the circumstances as stated in the question, then you should configure the "Type of VPN server I am calling" to be PPTP.

Incorrect answers:

A: MS-CHAP is only the authentication mechanism and this will not be the most secure connection type under the circumstances.

B: There is no need to specify a TCP/IP address in the Network properties.

C: Optional Encryption is not the most secure since there will be choices to use encryption or not.

D: Automatic Type of VPN server I am calling setting will be unnecessarily risky.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lessons 1 & 2

QUESTION 207

You install Windows 2000 Professional on your computer at home. You create a new dial-up connection to connect to your company's remote access server. You configure the connection to use both of your external modems and to use Multilink to bind the modems together.

You start the dial-up connection to connect to the remote access server. You notice that only one of the modems is connected to the remote access server.

What should you do?

A. Configure the dial-up connection to use a SLIP connection.

B. Configure the company's remote access server to accept Multilink connections.

C. Replace your modems with new modems that support Multilink.

D. Grant your user account Multilink permission on the company's remote access server.

Answer: B

Explanation: To use multilink modems, multilink must be enabled at the client and at the server. In the scenario, multilink is enabled at the client only. You therefore need to enable it at the server as well.

Incorrect answers:

A: SLIP is a legacy protocol. It can only be used on servers. It enables a remote connection from a Windows 2000 Server to a UNIX server, which cannot handle PPP.

C: Multilink is a feature of Windows 2000; it is not a feature of modems. All modems can be used in a Multilink connection.

D: There is no such thing as a Multilink permission in Windows 2000.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 1

QUESTION 208

You install Windows 2000 Professional on your portable computer. You create a new dial up connection to connect to your company's remote access server. You connect to the remote access server by using the dial up connection. You can connect to the servers on the same segment as the remote access server. You cannot access the shared resources that are on the remote segments from the remote access server.

What should you do?

- A. Configure the company remote access server to accept multilink connections.
- B. Configure the TCP/IP program for the dial up connection to disable IP header compression.
- C. Configure the TCP/IP properties for the dial up connection to use the default gateway on the remote network.
- D. Grant your user account dial in permission on the company remote access server.

Answer: C

Explanation: If the RAS client does not use the same Default Gateway as the RAS server, it will be able to reach the computers on the same segment as the RAS server, but it will not be able to reach other remote segments.

Incorrect answers:

A: This is not a multilink problem. A multilink problem is when not all communication lines are used.

B: Disabling header compression can be used when the dial-client and the dial-server are not able to communicate. This will enable the dial-client and the dial-server to communicate. It will not however, allow the client to reach other remote segments.

D: The client has successfully accessed to the RAS server. Therefore there cannot be a dial-in permission problem in this scenario.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 1

QUESTION 209

You are the network administrator for Certkiller . Laura is a sales representative for the company. She travels on a regular basis and dials into the company network from her Windows 2000 Professional portable computer. Certkiller recently implemented a new computing security policy that mandates all remote connections be established by a two-way authentication method. You configure a Windows 2000 Server computer to run Routing and Remote Access Server for Windows 2000 to meet the requirements of the new security policy. Laura reports she now cannot initiate a dial-up connection. Laura needs to dial in to the company network. What should you do?

- A. Apply the Hisecws.inf Security Template to Laura's computer.
- B. Apply the Compatws.inf Security Template to Laura's computer.
- C. Instruct Laura to configure her dial-up connection to use multi-link.
- D. Instruct Laura to configure her dial-up connection to use MS-CHAP v2.
- E. Instruct Laura to configure her dial-up connections to use L2TP.

Answer: D

Explanation: It seems that the new security policy on the RRAS server is preventing Laura from initiating dialin access. The security policy requires two-way authentication. MS-CHAP V2 supports two-way authentication. It would most likely enable Laura to connect.

Incorrect Answers

- A: The Hisecws.inf would increase the security on Laura's computer. However, increasing security would make it harder to connect.
- B: The Compatws.inf security policy would not help with the remote access. It is the security policy at the RRAS server that is the restriction, not the local security settings on Laura's computer.
- C: Multilink would enable faster communication, but it would not make it easier to initiate a dial-up connection.
- E: Setting up a tunneling is not required, and it would not do much good.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 1

QUESTION 210

You are the network administrator for Certkiller .

You install Windows 2000 Professional on your computer at home. Your computer contains three modems, each connected to a separate phone line. You create a new dial-up connection to connect to Certkiller 's remote access server. You configure the connection to dial up all three devices. You start the dial-up connection and connect to the remote access server. You notice that only one of the modems is

070-210

connected to the remote access server.

You want to use as many modems as possible to make a single connection to the remote access server. What should you do?

- A. Configure the dial-up connection to use a SLIP connection.
- B. Configure all three modems to use the same phone line.
- C. Configure the remote access server to enable multi-link.
- D. Configure the dial-up connection to only dial two of the three modems.
- E. Configure the dial-up connection to Enable LCP extensions.

Answer: C

Explanation: A multi-link connection is where multiple connections are combined into one to increase the bandwidth of the connection. To use multi-link, multi-link must be configured on the client computer and the remote access server.

Incorrect Answers:

A: SLIP is a legacy protocol used in old UNIX environments. SLIP is rarely used nowadays and has been superseded by PPP.

B: The modems need to use separate phone lines.

D: Multilink connections can use more than two modems.

E: LCP extensions are not required for multilink connections.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 1

QUESTION 211

You are the administrator of your company's network. Your network consists of 20 Windows 2000 Professional computers. You want to configure all of the computers to allow access to the Internet. Your budget does not allow for installing a permanent Internet connection for the network. You do have a single dial-up account at a local Internet Service Provider (ISP) and a 56-Kbps modem. You want the computer to be able to access the Internet when Web resources are requested. What should you do? (Choose all that apply)

- A. Configure the shared modem to use software handshaking
- B. Configure the dial-up connection to enable on-demand dialing.
- C. Configure the dial-up connection to enable the Internet Connection Sharing.
- D. Configure all the other computers to have a dial-up connection that uses the shared modem.
- E. Attach the modem to one of the Windows 2000 Professional computers, and create a dial-up connection to the ISP.
- F. Attach the modem to one of the Windows 2000 Professional computers, and share the modem on the

network.

Answer: B, C, E

Explanation: To enable the computer to access the Internet when Web resources are requested, you must first attach the modem to the computer and create a dial-up connection to the ISP. You must then configure the dialup

connection to enable Internet Connection Sharing. This can be accomplished by opening Network And Dial-Up Connections, then right-click the dial-up connection, select Properties, select the Sharing tab, and finally enable the Internet Connection Sharing For This Connection check box. To enable this connection to dial automatically when another computer on the home network attempts to access external resources, the Enable On-Demand Dialing check box must be selected.

Incorrect answers:

A: Software handshaking settings of the modem do not need to be configured when using Internet Connection Sharing.

D: The ICS clients on the network will not access the modem directly. They will access the ICS computer's shared Internet connection.

F: The Internet connection is shared, not the modem. Therefore the modem does not need to be shared.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 3

QUESTION 212

You use a Windows 2000 Professional portable computer both at the office and at home. In the office you connect the portable computer to a docking station and use Internet Explorer to access the Internet through your LAN connection.

At home, you configure a new dial-up connection to the Internet. Now when you attempt to access the Internet from the office you are prompted to connect via your dial-up connection. When you cancel this message, you can only work offline and cannot access the Internet.

You want to maintain your dial-up connection for home use and your ability to access the Internet when connected to the company LAN. What should you do?

- A. Reconfigure the dial-up connection to dial-up to a private network.
- B. Create another connection that uses a virtual private network (VPN) to connect to a private network through the Internet.
- C. Configure Internet Explorer to automatically detect proxy settings.
- D. Configure Internet Explorer to dial whenever a network connection is not present.

Answer: D

Explanation: Internet Explorer can be configured dial whenever a network connection is not present. This is exactly what is needed in this scenario.

Incorrect Answers:

A: Reconfiguring the dial-up connection to dial-up to a private network would not help.

B: We don't want to set up a VPN. We just want to have Internet access both at home and at the office.

C: There is no proxy server mentioned. Furthermore it would not prevent Internet Explorer from dialing.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 3

QUESTION 213

You are the network administrator for Certkiller .

You create a dial-up connection to your Internet service provider (ISP). You configure the dial-up connection Security tab as shown in the Dial-up Security Dialog Box.



You attempt to connect to the ISP. You view the status change from Dialing to Verifying user name and password. After several seconds, the status changes to Disconnecting. You are then disconnected from the computer you dialed. You verify that your user name and password are entered correctly.

You want to enable your computer to connect to your ISP.

What should you do?

Answer:



Explanation: if the setting is configured as "Allow unsecured password" then your computer will be able to connect to the ISP. It is already stated that you verified that the user name and password had been entered correctly.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 3

QUESTION 214

You are creating a shared Internet connection on your Windows 2000 Professional computer. You want to enable other computers on the LAN to be able to access only HTTP and FTP sites on the Internet. What should you do? (Choose all that apply)

- A. Configure your shared Internet connection to disable LCP extensions.
- B. Configure your shared Internet connection to disable on-demand dialing.
- C. Create an Internet Connection Sharing application type for HTTP to use remote server for port 25.
- D. Create an Internet Connection Sharing application type for HTTP to use remote server port 80.
- E. Create the Internet Connection Sharing application type for FTP to use remote server port 21.
- F. Create an Internet Connection Sharing application type for FTP to use remote server port 72.

Answer: D, E

Explanation: HTTP traffic uses TCP port 80 and FTP traffic uses TCP port 21 for session control and port 20 for data transfer. Therefore, by enabling TCP port 80 and TCP port 21 only HTTP and FTP traffic will be allowed. All other network traffic will not be allowed.

Incorrect answers:

A: LCP extensions are used in the context of RRAS and PPP. It is not used to prevent or allow any specific type of network traffic.

B: Disabling on-demand dialing on the shared Internet connection will not prevent network traffic. It will only prevent ICS clients initiating an Internet connection.

C: HTTP uses TCP port 80, not TCP port 25. FTP also does not use TCP port 25. It uses TCP ports 20 and 21. SMTP uses TCP port 25.

F: Neither FTP nor HTTP use port 72.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

QUESTION 215

Your desktop computer has Windows 2000 Professional installed. You create a new dial-up connection to connect to the Internet. You configure the Internet connection to enable Internet Connection Sharing. After you configure the connection, you cannot see or connect to any shared resources. You want your computer to be able to connect to shared resources.

What should you do?

- A. Configure the dial-up connection to disable shared access.
- B. Configure the dial-up connection to disable on-demand dialing.
- C. Disable data encryption in the new dial-up connection.
- D. Use the ipconfig command to release and renew your network TCP/IP address.

Answer: D

Explanation: When ICS is configured, the IP address for the ICS internal adapter changes to 192.168.0.1 with a subnet mask of 255.255.0.0. The other clients in the local network still have their old IP addresses. If their IP addresses are released and renewed they will get a correct IP configuration from the mini-DHCP server, which is included in ICS. The ICS clients would get IP addresses in the range of 192.168.0.2-192.168.0.254 and a subnet mask of 255.255.0.0. They would be able to communicate amongst themselves.

Incorrect Answers:

A: This would disable the ICS. As you want to keep the Internet Connection sharing, this would not be a good solution.

B: Disabling on-demand dialing prevents the ICS client computers from establishing an Internet connection. This might not be a good solution since this is a dial-up connection. Furthermore, this will not solve the problem in this scenario.

C: Data encryption settings on the dial-up would not cause any problems with local shares. Therefore, this solution will not solve the problem.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 21

QUESTION 216

You are the administrator of a Windows 2000 network. You install Windows 2000 Professional on a new computer and configure the TCP/IP settings to have a static IP address.

While testing network connectivity from the new computer, you discover an error in the DNS server address that is configured in the TCP/IP settings. You configure the correct DNS server address, which is 10.1.1.5. However, you are still unable to successfully connect to network resources by name.

You run the IPconfig /all command. The results indicate that the DNS server address is now configured as 0.0.0.0

You need to ensure that the computer can connect to network resources by name. What should you do?

- A. Stop and restart the DNS Client service.
- B. Add 10.1.1.5 to the DNS server list on the TCP/IP Advanced Properties tab.
- C. Add an A (host) record for the computer to the DNS server's zone file.
- D. Configure your DHCP server to have a DNS server address of 10.1.1.5.

Answer: A

Explanation: In this scenario the client computer does not have the correct information in its local DNS cache. There are two ways to solve this problem. You could use ipconfig /flushdns to reset the DNS cache, or you could stop and restart the DNS client service.

Incorrect answers:

B: The correct DNS address is already configured. When you enter a preferred DNS Server IP address, this address is automatically added in the DNS server list on the TCP/IP Advanced properties tab. The DNS Server list is used to add more than 2 DNS servers.

C: The client cannot find the DNS server. Adding an A (host) record for the client computer would only help other computer to find the client computer but will not enable the client to find the DNS server. This solution is thus not appropriate to the problem in this scenario.

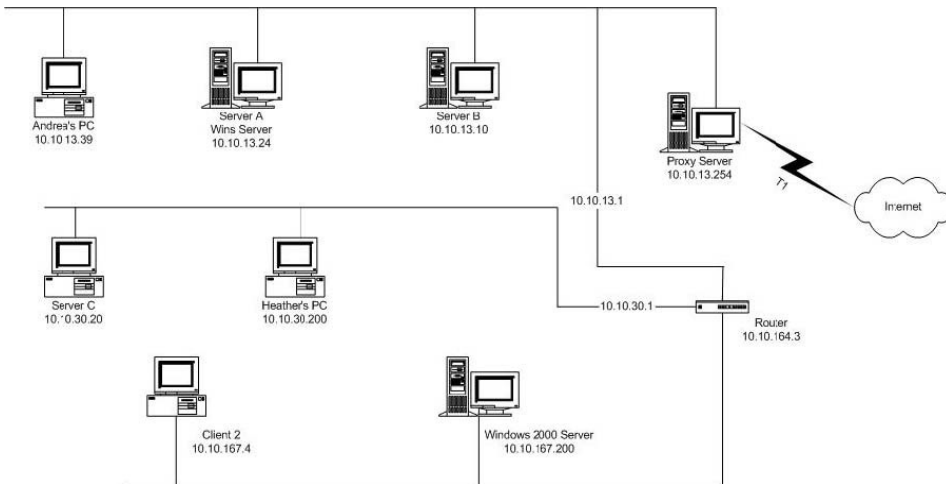
D: The client computer has a static IP address and does not use a DHCP server to for IP configuration information. Therefore, changing the DNS server's IP address in the DHCP is in appropriate.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 8, Lesson 3

QUESTION 217

You install Windows 2000 Professional on a computer named Client2. The network configuration is shown in the exhibit. .



You connect to the shared resources on ServerC daily. Today, you cannot connect to ServerC. Heather can connect to ServerC successfully from her computer. You ping ServerC to find out the nature of the problem as shown in the Ping results exhibit. .

```

c:\C:\WINDOWS\System32\cmd.exe
c:\>ping serverC

Pinging serverc.amraf.com [10.10.30.20] with 32 bytes of data:

Reply from 10.10.164.3: Destination host unreachable.
Reply from 10.10.164.3: Destination host unreachable.
Reply from 10.10.164.3: Destination host unreachable.
Reply from 10.10.164.3: Destination host unreachable.

Ping statistics for 10.10.30.20:
    Packets: Sent = 4, Recieved = 4, Lost = 0 <0% Loss>,
    Approximate round trip in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

You verify that all of the servers are connected to the network and are running correctly. What is the most likely cause of the problem?

- A. The router configuration.
- B. The WINS configuration on Client2.
- C. The WINS configuration on ServerC.
- D. The default gateway setting on Client2.

Answer: A

Explanation: The servers on the various network segments can communicate with servers on the same network segment. Therefore the problem must lay with the router configuration, since communication across the router is not successful.

Incorrect Answers:

B: In the exhibit you see "Reply from 10.10.164.3: Destination host unreachable". This shows that Client2 communicates with the Router, which is the Default Gateway. So the WINS configuration on Client2 is not the cause of the problem.

C: Heather, who is on the same subnet as ServerC, is able to communicate with ServerC. Therefore there is no WINS configuration problem on ServerC.

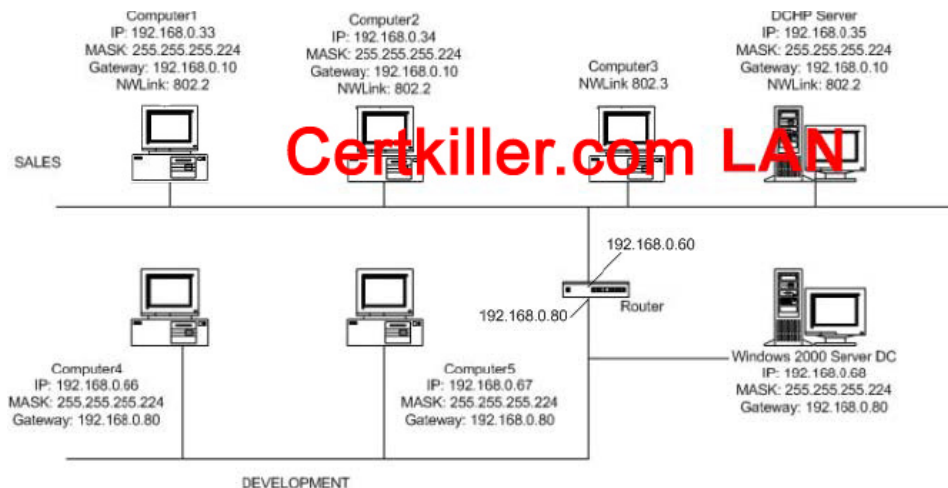
D: Client2 does communicate with the Default Gateway (the Router in this case). You see this in the exhibit: the replies from 10.10.164.3

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 22

QUESTION 218

You are the administrator of a Windows 2000 network. The network is configured as shown in the exhibit.



Computers on the Sales subnet run Windows 2000 Professional. These computers are dynamically assigned IP addressing and configuration information from a DHCP server on the subnet.

Computers on the development subnet run Windows 98. These computers are statically assigned IP addressing and configuration information.

Users on the Sales subnet report that they cannot communicate with users on the development subnet. A user who works on computer3 reports that he cannot communicate with computers on either subnet. You want all users to be able to communicate with other users on both subnets.

What should you do? (Choose two)

- A. Change the frame type to 802.2 on computer3.
- B. Change the default gateway option IP address on the DHCP server.
- C. Change the default protocol on the computers on the Sales subnet to NWLink IPX/SPX/NetBIOS Compatible Transport Protocol.
- D. Enable TCP/IP protocol with the default settings on Computer3.
- E. Add the NetBEUI protocol to the binding order on all client computers.

Answer: B, D

Explanation: The computers on the Sales subnet cannot communicate with any computers on the development subnet, but they communicate with each other with the exception of computer3, which cannot communicate at all. An incorrect default gateway address on the computers within the Sales subnet explains why they cannot communicate with the development subnet. This problem is resolved by changing the default gateway option on the DHCP server. Computer3 needs to be configured with the TCP/IP protocol to be able to communicate with the other computers.

Incorrect answers:

A: Changing the frame type to 802.2 on computer3 would allow computer3 to communicate with the other computers on the Sales subnet, but it would not allow communication with the computers on the development subnet which all use TCP/IP.

C: Changing the default protocol to NWLINK on the Sales subnet would not allow them to communicate with the development TCP/IP-configured computers.

E: NetBEUI is not a routable protocol. It would not allow communication between any of the subnets.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 8, Lessons 1 & 2

QUESTION 219

Your routed TCP/IP network consists of 10 Windows 2000 Server computers and 75 Windows 2000 Professional computers. Your network uses TCP/IP as the only network protocol. You are installing 10 new Windows 2000 Professional computers. You want to enable the new computers to use NetBIOS names to connect to all shared resources as the network. You configure a TCP/IP address and a subnet mask on each new computer.

Which 2 additional TCP/IP properties should you configure on each new computer? (Choose two)

- A. The bindings.
- B. A DNS address.
- C. A Gateway address.
- D. A WINS server address.
- E. A DHCP server address.

Answer: C, D

Explanation: As the network is routed, it consists of more than one subnet. On a routed network a default gateway address has to be configured so that the clients on one subnet will be able to communicate with the clients on another subnet across the router. The requirement to use NetBIOS names in a routed environment forces us to use a WINS server, as NetBIOS broadcasts cannot pass across the router.

Incorrect answers:

A: There is no bindings option in TCP/IP properties.

B: There is a requirement to use NetBIOS names. WINS is used for NetBIOS names while DNS is used for

domain name resolution.

E: An IP address and subnet mask is already configured on all clients.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 22

QUESTION 220

You install Windows 2000 Professional on a computer named client2. Client2 is configured to have a TCP/IP address of 10.10.167.4 and a default gateway of 10.10.167.1.

The network is configured as shown in the exhibit.

You want to connect to a shared folder on server B. You want to attempt to connect to the network share.

You receive the following error message, 'the network location cannot be reached'. You run ipconfig to view the configuration on client 2. Which configuration setting would you change?

(To answer, click the incorrectly configured network setting in the IP configuration display.)

```
Windows 2000 IP Configuration

Host Name . . . . . : Client2
Primary DNS Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . :

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . :

Physical Address. . . . . : 00-08-c7-c3-13-c4
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 10.10.167.4
Subnet Mask . . . . . : 255.255.255.252
Default Gateway . . . . . : 10.10.167.1
DHCP Server . . . . . : 10.10.13.20
Primary WINS Server . . . . . : 10.10.13.20
Secondary WINS Server . . . . . : 10.20.13.20

Lease Obtained. . . . . : Tuesday, December
```

Answer: Subnet mask

Explanation: The subnet mask is too restrictive. It must include more nodes.

Incorrect answers:

The configuration of the Default Gateway does not need to be changed.

The advanced option does not need to be used.

Reference:

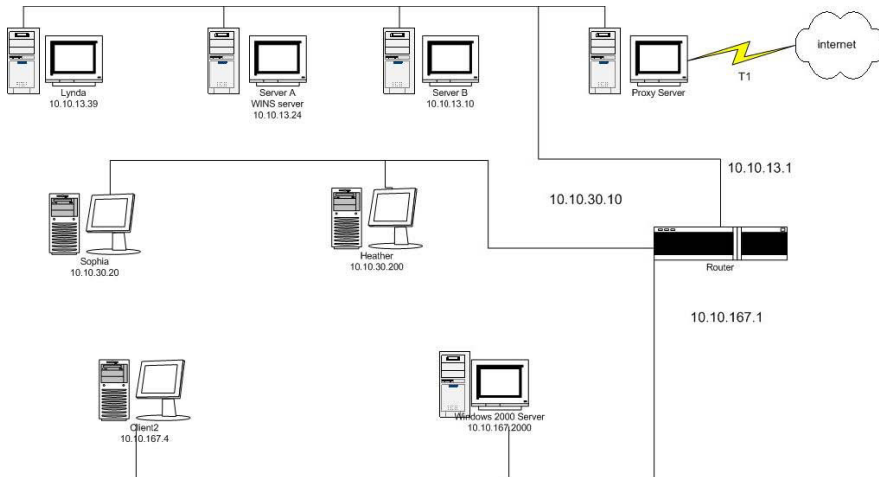
Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 8

QUESTION 221

You install Windows 2000 Professional on a computer named Client2. The computer is configured to have a TCP/IP address of 10.10.167.4 and a default gateway of 10.10.167.1

You want to connect to a shared folder on a server B. When you attempt to connect to the network share you receive the following error message, 'the network location could not be reached'.

The network diagram is shown in the exhibit.



You want to allow Client2 to connect to server B. What should you do?

- A. Place Client2 on the same segment as server B.
- B. Place a computer running the WINS proxy on the same segment as Client2.
- C. Configure Client2 to use a default gateway of 10.10.13.1.
- D. Configure Client2 use a DNS server address of 10.10.13.24.
- E. Configure Client2 to use a WINS server address of 10.10.13.24.

Answer: E

Explanation: Client2's default gateway setting, the IP address, 10.10.167.1, of the Router's local interface is correct. Client2 requires a name resolving service to be able to use names to connect to resources, such as ServerB, on the network. The only name resolution service provided by the network is the WINS server named Server A, which has an IP address of 10.10.13.24. By configuring Client2 with the WINS server address of 10.10.13.24, Client2 will be able to connect to Server B.

Incorrect answers:

- A: Placing Client2 on the same segment as server B should not be necessary, as Client2 has been provided with the correct default gateway IP address of 10.10.167.1.
- B: A WINS proxy is used for clients with operating systems that do not support WINS. Windows 2000 Professional support WINS so there is no need for a WINS proxy.
- C: Client2 has been provided with the correct default gateway IP address of 10.10.167.1. The IP address of

10.10.13.1 is the IP address of the Router's remote interface. The default gateway should be configured with the IP address of the local interface of the Router, which is 10.10.167.1.

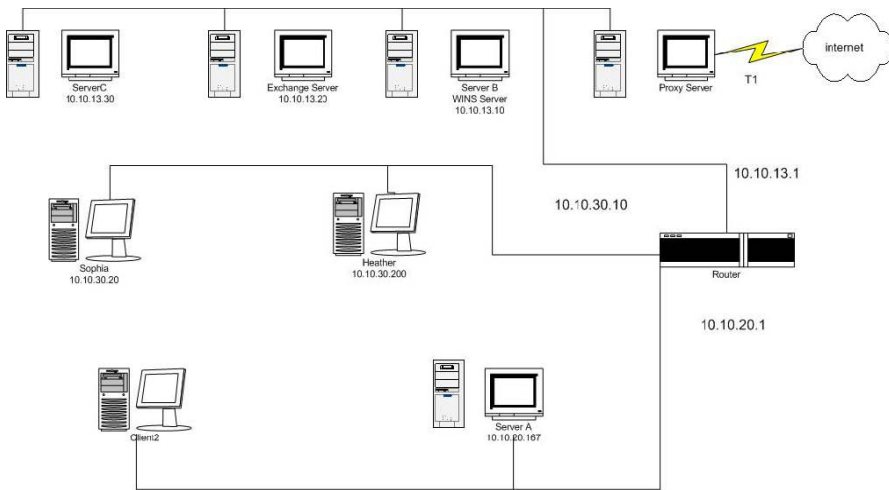
D: There is no DNS server on the network. Server A, the WINS server, has the IP address 10.10.13.24.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 22

QUESTION 222

You are installing Windows 2000 Professional on a computer named client2. The network is configured as shown in the exhibit.



Your network uses TCP/IP as the only network protocol. You configure Client2 to have a TCP/IP address of 10.10.20.234, a default gateway of 10.10.13.1, and a WINS Server address of 10.10.13.10. ServerB is configured with TCP/IP. ServerB is the network WINS server.

You cannot connect to shared resources on ServerB and ServerC by using UNC names. You want Client2 to be able to connect to ServerB and ServerC.

What should you do?

- A. Configure Client2 to use a default gateway of 10.10.20.1.
- B. Configure Client2 to use a TCP/IP address of 10.10.13.234.
- C. Install a WINS server on the same segment as Client2.
- D. Install and configure a DNS server, and configure Client2 to use the DNS server service.

Answer: A

Explanation: The exhibit indicates that Client2 has an incorrect default gateway setting. From the exhibit we see that:

10.10.20.1 is the IP address of the internal interface of the Router.

10.10.13.1 is the IP address of the external interface of the Router.

The internal (local) interface (10.10.20.1) of the Router should be used as a default gateway.

Incorrect answers:

B: There is no need to change the TCP/IP address of Client2. This will not enable Client2 to connect to ServerB. You should instead configure Client2 with the correct the default gateway.

C: It is not necessary to install a WINS server on the same segment as Client2. Client2 would be able to reach the WINS server on the other segment if the default gateway setting was configured correctly. Furthermore, adding a WINS server to the segment that Client2 is on will not enable Client2 to connect to ServerB.

D: Client2 is already configured for WINS therefore DNS is not required as WINS and DNS are both responsible for name resolution, and both can be used by Windows 2000 Professional.

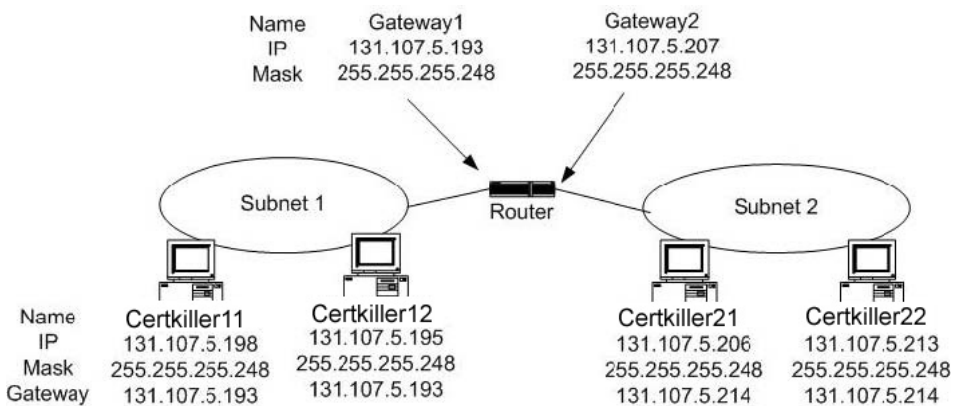
Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 22

QUESTION 223

You are the network administrator for Certkiller . You are configuring a network consisting of 100 client computers and six subnets for Certkiller 's new office. You configure the first two subnets and configure client computers on both subnets for testing. You test the initial configuration and discover that not all of the client computers can communicate with each other.

The two subnets are show in the following diagram.



All client computers must be able to communicate with each other. What should you do?

- A. Change the subnet mask of all the client computers and on the two gateways to 255.255.255.240.
- B. Change the subnet mask of all the client computers and on the two gateways to 255.255.255.255.
- C. Change the IP address for Gateway2 to 131.107.5.214 and the IP address for Certkiller 21 to 131.107.5.210.
- D. Change the IP address for Certkiller 11 to 131.107.5.190 and the IP address for Certkiller 12 to 131.107.5.191.

Answer: C

Explanation: Certkiller 21 and Certkiller 22 on subnet 2 use the default gateway of 131.107.5.214, while Gateway2 currently has the IP address of 131.107.5.207. We must make these settings match. For example, by

changing the IP address of Gateway2 to 131.107.5.214.

Furthermore, the IP address of Certkiller 21 belongs to another subnet than Certkiller 22 and Gateway2. We must

adjust the IP address of Certkiller 21.

Incorrect Answers

A: The configured subnet masks are OK. All clients and both the network adapters on the router have the same network mask.

B: The subnet masks are OK. Furthermore, the subnet mask 255.255.255.255 should not be used.

D: There is no need to change the IP address of Certkiller 11 or Certkiller 12. They belong to the same subnet as Gateway2 already.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 22

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 7, Lesson 1 & Chapter 8

QUESTION 224

You are the network administrator for Certkiller . You manage Windows 2000 Professional computers on four subnets and Windows 2000 Server computers on a dedicated subnet. All of the client computers are configured as DHCP clients.

You receive a call from Andrew who cannot access a file server. You run the ipconfig /all command from Andrew's computer. The results are shown in the exhibit.

```
D:\WINNT\System32\CMD.exe
D:\>ipconfig /all

Windows 2000 IP Configuration

    Host Name . . . . . : kaballen
    Primary DNS Suffix . . . . . :
    Node Type . . . . . : Broadcast
    IP Routing Enabled. . . . . : Yes
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : SMC EZ Card 10/100 <SMC1211TX>
    Physical Address. . . . . : 00-E0-29-47-BF-48
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Autoconfiguration IP Address. . . . . : 169.254.72.166
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :
    DNS Servers . . . . . :
```

Other client computers on the same subnet can connect to the file server. You confirm that the DHCP service is operating correctly.

You need to help Andrew connect to the file server. What should you do?

- A. Configure the routers to forward BOOTP traffic.
- B. Add IP addresses to the appropriate scope in the DHCP server.
- C. Run the net start DHCP command on Andrew's client computer.
- D. Configure a default gateway of 169.154.72.1 on Andrew's client computer.
- E. Configure a LMHOSTS file entry for the file server on Andrew's client computer.

Answer: B

Explanation: The exhibit shows that Andrew's computer has been self-configured with an APIPA address, an address in the 169.254.xx.xx range. His computer has not been able to receive IP configuration from a DHCP server. This is the reason he cannot access the file server.

It is plausible, but not very likely, that the DHCP server has run out of IP addresses to lease. However, this is the only possible cause in this scenario (see incorrect answers). We should therefore add more IP addresses to the DHCP scope. Andrew's computer would then be able to lease a proper IP address, and would be able to access the file server.

Incorrect Answers

A: If the router were blocking BOOTP traffic no clients on Andrew's subnet would receive any IP configuration. But all client computers are DHCP clients and all clients are able to access the file server, so the router is forwarding BOOTP traffic already.

C: Andrew's computer is a client. There is no need to run the DHCP server service on a client.

D: Addresses in the 169.254.xx.xx range are APIPA addresses. It is highly unlikely that they are in use on the network.

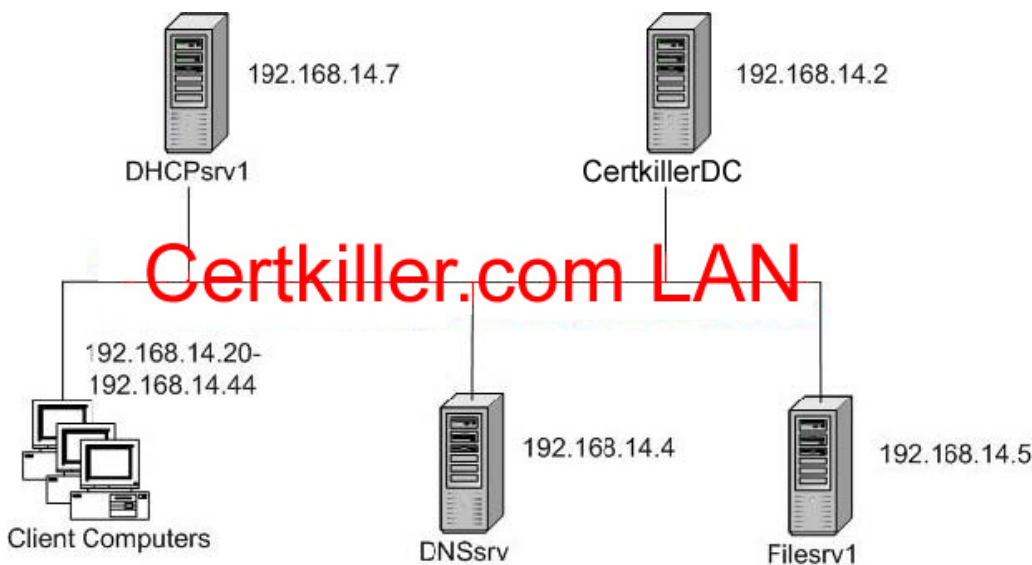
E: This is an IP configuration problem, not a name resolution problem.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 8, Lesson 1

QUESTION 225

You are the network administrator for a Certkiller . Your network consists of 25 Windows 2000 Professional client computers and four Windows 2000 Server computers in a native-mode Windows 2000 domain. All of the computers are on a single subnet. The client computers are configured for dynamic IP address allocation. The network is configured as shown in the exhibit.



A developer named Julia reports that she cannot connect to file server Filesrv1 from her client computer

named Computer22. When she attempts to browse \\Filesrv1 from the Run line she receives the message, "The network path was not found". No other users are reporting problems connecting to Filesrv1. From Julia's client computer, you browse \\192.168.14.5 from the Run line and successfully connect to the server. You run the ipconfig /all command. The relevant results are shown in the following table.

Host Name	CertKiller22
DHCP Enabled	Yes
IP Address	192.168.14.42
Subnet Mask	255.255.255.0
Default Gateway	(not configured)
DHCP Server	192.168.14.7
DNS Server	192.168.14.7
WINS Server	(not configured)
Node Type	Peer-peer

You want Julia to be able to access resources on Filesrv1 by using the computer name. What should you do?

- A. Configure the client computer with a default gateway of 192.168.14.2.
- B. Configure the client computer with a subnet mask of 255.255.0.0.
- C. On the Internet Protocol (TCP/IP) Properties sheet, select the Obtain DNS server address automatically option.
- D. On the Internet Protocol (TCP/IP) Properties sheet, select the Obtain an IP address automatically option.

Answer: C

Explanation: The computer obtains its IP address and subnet mask automatically, but the DNS server address is statically configured. The DNS server configuration is incorrect. It should be set to 192.168.14.4 not 192.168.14.7. We could either do this statically, or by enabling the DHCP server to configure the DNS address.

Incorrect Answers

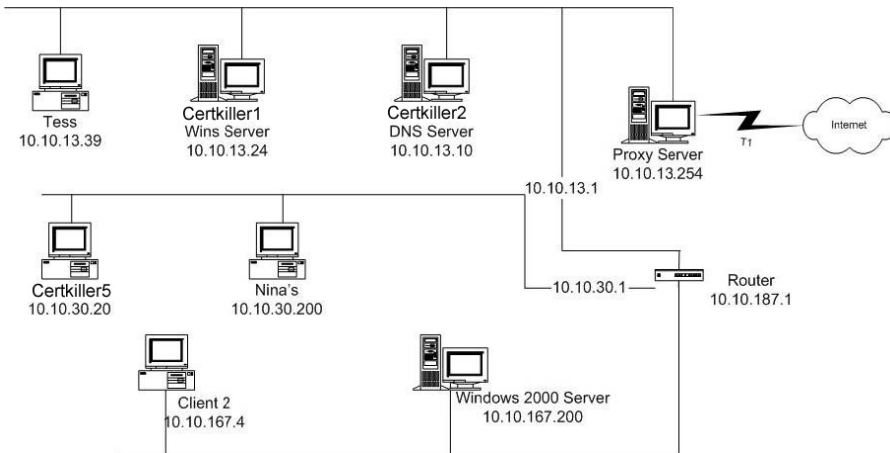
- A: There is only one subnet in the network so no default gateway is required.
- B: It is not an IP configuration problem. Julia can access Filesrv1 using an IP address.
- D: The computer is already configured to obtain an IP address automatically. This can be seen in the second exhibit which states that DHCP is enabled.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 8, Lesson 3

QUESTION 226

You are the administrator of Certkiller 's network. You install Windows 2000 Professional on a computer named Client2. The network is configured as shown in the Network Configuration exhibit.



You attempt to connect to a Web server on the Internet. You cannot connect by using the Web server's URL. You can connect to the Web server by using its TCP/IP address. You run IPConfig to review the configuration as shown in the IP Configuration exhibit.

```

C:\WINNT\System32\cmd.exe
C:\>ipconfig /all

Windows 2000 IP Configuration

Host Name . . . . . : CLIENT2
Mode Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : 
   Description . . . . . : Compaq Integrated NetFlex-3/P Controlle
   r 2.3
   Physical Address. . . . . : 00-08-C7-C3-13-C4
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IP Address . . . . . : 10.10.167.4
   Subnet Mask . . . . . : 255.255.252.0
   Default Gateway . . . . . : 10.10.167.1
   DHCP Server . . . . . : 10.10.13.20
   Primary WINS Server . . . . . : 10.10.13.20
   Secondary WINS Server . . . . . : 10.20.13.20
   Lease Obtained. . . . . : Monday, August 02, 1999 8:41:00 AM
   Lease Expires . . . . . : Thursday, August 12, 1999 8:41:00 AM

```

You want to enable Client2 to connect to Web servers by using URLs. What should you do?

- A. Configure your computer to use Certkiller 1 as a proxy server.
- B. Configure your computer to use Certkiller 1 as a WINS server.
- C. Configure your computer to use Certkiller 2 as a DNS server.
- D. Configure your computer to use Certkiller 2 as a default gateway.

Answer: C

Explanation: You are able to access the Web server by using the TCP/IP address, but not by using the host name. This indicates that there is a name resolution problem. As your computer is running Windows 2000 Professional we should configure it with a proper DNS server.

Incorrect Answers

A: A proxy server would not be of any use in this scenario.

B: Windows 2000 does not use ordinarily WINS for name resolution. Furthermore, to be able to resolve fully qualified names used in URLs DNS, not WINS, is required.

D: The local interface of the router is already correctly configured as the default gateway.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 8, Lesson 3

QUESTION 227

The network at Certkiller Ltd. consists of one Windows NT Server 4.0 domain and 35 Windows 2000 Professional computers. The Certkiller network consists of five interconnected TCP/IP subnets. All of the computers use TCP/IP as the only network protocol.

You are adding 15 Windows 2000 Professional computers to the network. You want to enable the Windows 2000 Professional computers to resolve NetBIOS names to TCP/IP addresses.

What should you do?

A. Install a DHCP server. Configure each computer to use DHCP.

B. Install a WINS server. Configure each computer to use WINS.

C. Create a Lmhosts.sam file on each computer. Add an entry containing the TCP/IP address and NetBIOS name for each computer on the network.

D. Create a Hosts.sam file on each computer. Add an entry containing the TCP/IP address and NetBIOS name for each computer on the network.

Answer: B

Explanation: The WINS network service is used to resolve NetBIOS names to TCP/IP addresses.

Incorrect Answers

A: A DHCP server is just used to automate IP configuration.

C: Lmhosts files can be used to resolve NetBIOS names to IP addresses. However, this is an awkward solution that requires extra administrative burden.

D: Hosts files are used to resolve Fully Qualified Domain Names, not NetBIOS names.

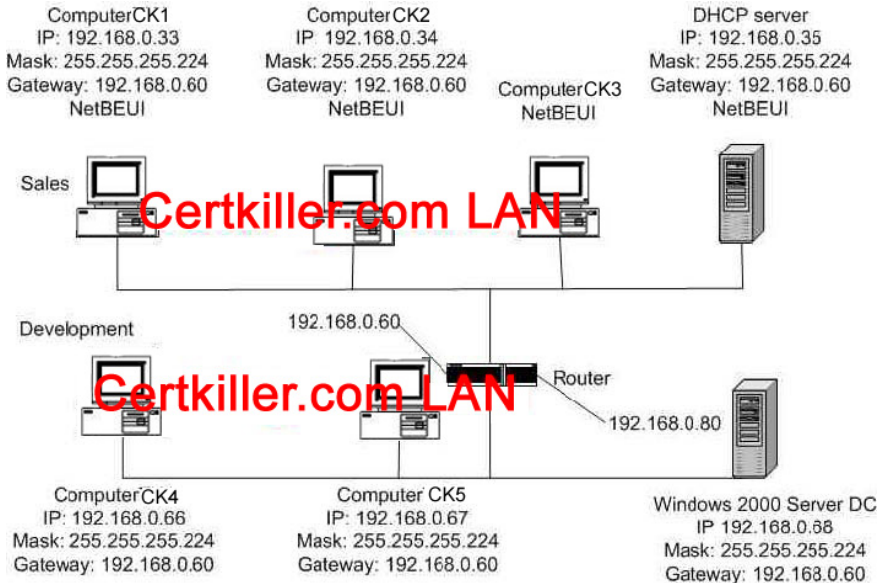
Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 8

QUESTION 228

You are the administrator of a Windows 2000 network. The network is configured as shown in the Network Diagram.

070-210



Client computers on the Sales subnet run Windows 98 and use DHCP. Client computers on the Development subnet run Windows 2000 Professional and use statically assigned TCP/IP settings. Users on the Sales subnet report that they cannot communicate with users on the Development subnet. A user who works on Computer CK3 reports that he cannot communicate with computers on the development subnet.

You want all users to be able to communicate with other users on both subnets. What should you do? (Each correct answer presents part of the solution. Choose two)

- A. Enable the NetBEUI protocol on all computers on both subnets.
- B. Enable the TCP/IP protocol with the default settings on Computer CK3 .
- C. Change the subnet mask on all computers to 255.255.255.0.
- D. Change the default gateway DHCP scope option to 192.168.0.80.
- E. Change the default gateway on the computers on the Development subnet to 192.168.0.80.

Answer: B, E

Explanation: NetBEUI is a non-routable protocol. Therefore, for Computer CK3 to communicate with computers in the Development subnet, it will need to be configured to use TCP/IP. The default setting for the TCP/IP protocol is to use DHCP. This is how the other computers in the Sales subnet are configured. The default gateway setting on the Development subnet computers is wrong. It should be set to the IP address of the local interface of the router; in this case 192.168.0.80.

Incorrect Answers:

- A: NetBEUI is a non-routable protocol so using it on all computers on both subnets won't solve the problem.
- C: The subnet mask on all the computers is valid. It does not need to be changed to 255.255.255.0.
- D: The DHCP scope is used by computers on the Sales subnet. The default gateway for the Sales computers should be 192.168.0.60, not 192.168.0.80.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 8

QUESTION 229

You are the network administrator for Certkiller .

Your network consists of one Windows NT Server 4.0 domain and 35 Windows 2000 Professional computers. The network consists of five interconnected TCP/IP subnets. All of the computers use TCP/IP as the only network protocol. You are adding 15 Windows 2000 Professional computers to the network. You configure each of the new computers to use DHCP. The computers can communicate with each other but are unable to communicate outside their own subnet. You run the ipconfig command to examine the IP address on one of the new computers. The IP address is 169.254.101.72

You want to enable the Windows 2000 Professional computers to communicate outside their own subnet. What should you do?

- A. Install a DHCP server.
- B. Install a WINS server. Configure each computer to use WINS.
- C. Create an Lmhost file on each computer.
- D. Create a Hosts file on each computer.

Answer: A

Explanation: A configured DHCP server provides a database of available IP addresses. The server can also be set up to provide configuration options for DHCP clients, including addresses of DNS and WINS servers, gateway addresses, and other information.

At startup, each DHCP client requests configuration data from the server, permitting automatic configuration of the IP address, subnet mask and other options. The IP address is assigned to each client for an amount of time determined at the server, called a lease, which can be periodically renewed. At conclusion of the lease, the client attempts to renew the lease, or the IP address is returned to the database and is made available to other DHCP clients. DHCP provides an efficient IP configuration option for larger networks, providing simplified client configuration, and reuse of IP addresses.

Thus if the new computers are configured to use DHCP and you want them to communicate outside their own subnet, then you should install a DHCP server.

Incorrect answers:

B: If you install a DHCP server, then installing a WINS server would be obsolete, furthermore, the new computers are already configured to use DHCP. So if you install a WINS server, then they will be excluded from communications.

C & D: Hosts and Lmhosts files provide host-to-IP and NetBIOS-to-IP name resolution via manually maintained local files; and b-node broadcasts, which can be used for NetBIOS name resolution within the local subnet. Hosts files are used to resolve Fully Qualified Domain Names, not NetBIOS names. HOST files map DNS entries. You must use DNS if you are using TCP/IP to communicate over the Internet or if your private internetwork uses DNS to resolve host names. Since the new computers are already configured to make use of DHCP, this option is not the solution if you want to enable them to communicate outside of their own subnet.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 8, Lessons 1, 2 & 3

QUESTION 230

You are the administrator of a Windows 2000 network. The network consists of a Windows 2000 domain named Certkiller .com.

You install Windows 2000 Professional on a new computer named CK1 and configure the TCP/IP settings to have a static IP address. You plan to join CK1 to the Certkiller .com domain. You configure two DNS server addresses in the TCP/IP properties. The first DNS server address is for a DNS server hosted by your ISP, the second DNS server address is for a DNS server authoritative for the Certkiller .com domain. When you attempt to join CK1 to the domain, you are unable to do so. You can successfully PING the IP address of each DNS server from CK1 .

You want CK1 to be able to join the Certkiller .com domain.

What should you do?

- A. Delete the second DNS server entry.
- B. Delete the first DNS server entry.
- C. Add an A (host) record for the computer to the appropriate DNS zone.
- D. Configure the computer to Obtain an IP address automatically.

Answer: B

Explanation: The Domain Name System (DNS) provides name-to-IP mapping by a distributed database. A Windows 2000 Professional-based client configured for DNS name resolution can query one or more DNS servers for name resolution services. Since you are unable to join CK1 to the domain, and is able to ping the IP address of each DNS server from CK1 ; and given that the first DNS server address is for the ISP, you should delete the first DNS server entry to join the Certkiller .com domain.

Incorrect answers:

A: The second DNS server entry is authoritative for the Certkiller .com domain which is necessary to be able to join the domain. Therefore you should not delete it.

C: Adding an A (host) record for the computer to the appropriate DNS zone does not guarantee the ability to join the domain.

D: Automatic IP addressing is done though the DHCP server.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 8, Lesson 3

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 22

QUESTION 231

You are the network administrator for Certkiller .

Your network is a native mode Windows 2000 domain consisting of 50 Windows 2000 Professional client

computers and six Windows 2000 Server computers. There are no routers on the network. The client computers have been configured for dynamic IP address application. The network is configured as shown in the Network Diagram.

MISSING

A user reports that she cannot connect to the server named CK1 from her client computer named Workstation5. When she attempts to browse \\ CK1 from the Run line she receives the message, "The network path was not found". No other users are reporting problems connecting to CK1 . From the user's computer, you browse \\192.168.72.6 from the Run line and successfully connect to the server. You run the ipconfig /all command. The relevant results are shown in the following table.

Host Name	Workstation5
DHCP Enabled	Yes
IP Address	192.168.72.42
Subnet Mask	255.255.255.0
Default Gateway	(not configured)
DHCP Server	192.168.72.5
DNS Server	192.168.72.5
WINS Server	(not configured)
Node Type	Peer-peer

You want the user to be able to access resources on CK1 by using the computer name. What should you do?

- A. On the Internet Protocol (TCP/IP) Properties sheet, select the Obtain DNS server address automatically option.
- B. On the Internet Protocol (TCP/IP) Properties sheet, select the Obtain an IP address automatically option.
- C. Configure the client computer with a default gateway of 192.168.0.1.
- D. Configure the client computer with a subnet mask of 255.255.0.0.
- E. Configure the client computer with a WINS server of 192.168.72.5

Answer: B

QUESTION 232

You are the administrator of Certkiller .com's network.

070-210

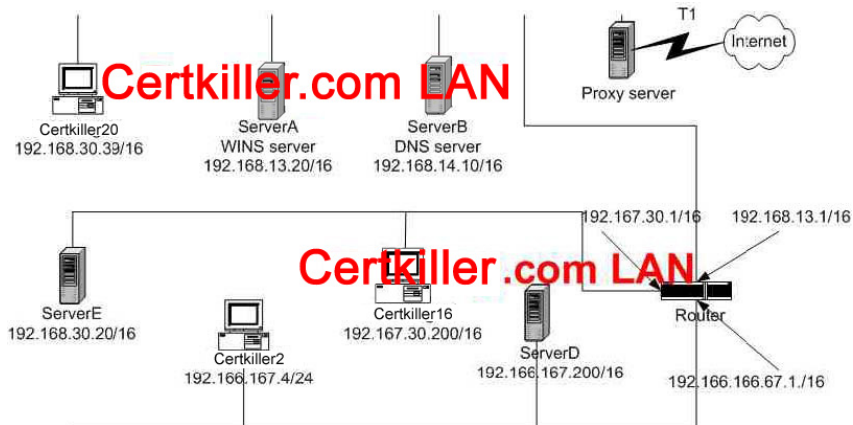
A user reports that he cannot access any resources on the Internet from his Windows 2000 Professional computer named Certkiller 2. You use Certkiller 20 and can connect to the Internet. You log on to Certkiller 2 and run the ipconfig /all command. The relevant results are shown in the following table.

Host Name	Certkiller 2
IP Address	192.166.167.4
Subnet Mask	255.255.255.0
Default Gateway	192.166.67.1
DHCP Enabled	No
DNS	192.168.14.10
WINS	192.168.12.30

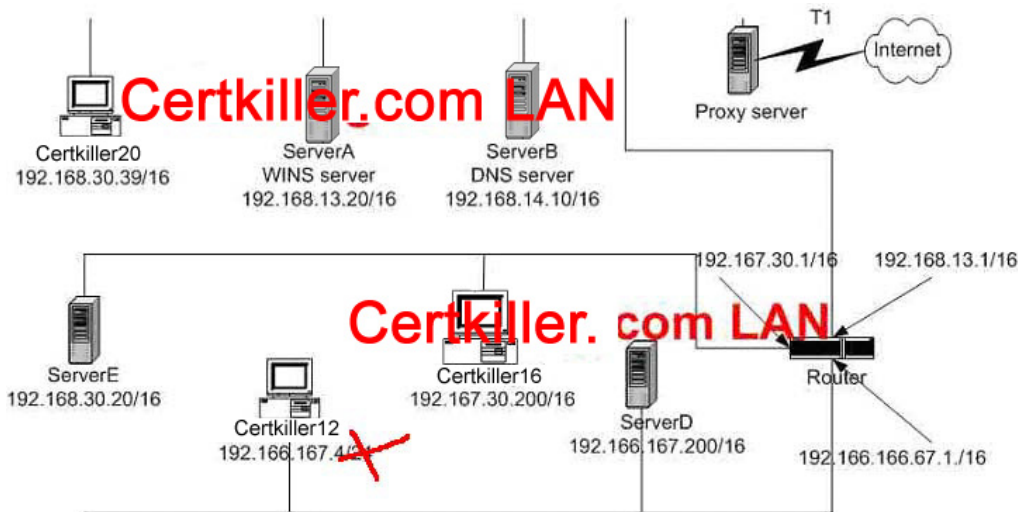
You want to be able to connect to the Internet from Certkiller 2. You also want to accomplish this task with the least amount of administrative effort.

What network configuration component or components should you modify?

To answer, select the appropriate network component or components in the Network Diagram.



Answer:

**QUESTION 233**

You are the administrator of Certkiller .com's Windows 2000 Network.

Your routed TCP/IP network consists of 10 Windows 2000 Server computers and 75 Windows 2000 Professional computers. All computers are in the Certkiller .com domain. Your network uses TCP/IP as the only network protocol. You are installing 10 new Windows 2000 Professional computers. You want to enable the new computers to use host names to connect to shared resources on the network. You configure a TCP/IP address, a gateway address and a subnet mask on each new computer.

You want to complete the configuration to allow the computers to communicate on the network.

What should you do? (Each correct answer presents complete solution. Choose two)

- A. Configure a HOSTS file.
- B. Configure a LMHOSTS file.
- C. Configure a WINS server database.
- D. Configure a DHCP server address.
- E. Configure at least one DNS address.

Answer: A, E

Explanation: Windows 2000 Professional provides four methods for resolving names to IP addresses:

(1) Domain Name System (DNS) for applications and services that require host-to-IP name resolution, such as Active Directory

(2) Windows Internet Name Service (WINS), for compatibility with applications and services that require NetBIOS-to-IP name resolution, such as browsing functions of previous versions of Windows

(3) Hosts and (4) Lmhosts files, which provide host-to-IP and NetBIOS-to-IP name resolution via manually maintained

local files; and b-node broadcasts, which can be used for NetBIOS name resolution within the local subnet.

070-210

Hosts files are used to resolve Fully Qualified Domain Names, not NetBIOS names. HOST files map DNS entries. You must use DNS if you are using TCP/IP to communicate over the Internet or if your private internetwork uses DNS to resolve host names. Therefore you should configure at least one DNS address. Then you would be able to allow communication on the network.

Incorrect answers:

B: If Lmhosts file is used, modify file and configure settings. For networks without access to a WINS name server, creation of an Lmhosts file can provide NetBIOS name resolution for application and services.

This file can also be used in an environment where name servers are available, but not all hosts are registered; for example, a server that is not available for general use, but is only to be accessed by a limited number of clients. This file must be manually created and updated as computer names and addresses change. Thus, Lmhosts files can be used to resolve NetBIOS names to IP addresses.

C: WINS provides name-to-IP resolution for applications and services using the NetBIOS command set for networks with a WINS server. The WINS network service is used to resolve NetBIOS names to TCP/IP addresses.

D: Windows 2000 Professional provides several different types of name resolution, including DNS, WINS, and name resolution using Hosts or Lmhosts files, and broadcast name resolution. Generally, a Windows 2000 Professional-based computer uses a combination of these name resolution types. But not DHCP server addresses. You need to determine if automatic configuration is available at the DHCP server.

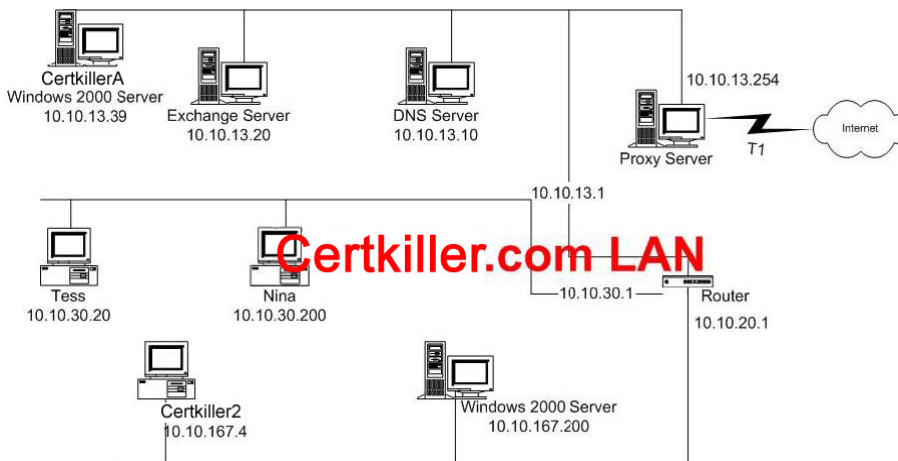
Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part IV, Chapter 22

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 21, Lesson 2

QUESTION 234

You are adding a Windows 2000 Professional computer named Certkiller 2 to the Certkiller company network. Your network consists of a single domain named Certkiller . Certkiller is configured as shown in the exhibit.



All of the computers use TCP/IP as the only network protocol. You want users on Certkiller 2 to access shared resources on Certkiller

A. You also want Certkiller 2 to be a member of the Certkiller domain.
What should you do? (Choose all that apply)

070-210

- A. Create an account for Certkiller 2 on Certkiller A.
- B. Create an account for Certkiller 2 in the Certkiller domain.
- C. Configure the router to support BOOTP.
- D. Configure Certkiller 2 to have an IP address of 10.10.20.78 and a default gateway of 10.10.20.1.
- E. Configure Certkiller 2 to have an IP address of 10.20.20.133 and a default gateway of 10.10.13.1.
- F. Configure Certkiller 2 to have an IP address of 10.10.30.200 and a default gateway of 10.10.20.1

Answer: B, D

Explanation:

B: Every client computer must be a member of the domain.

D: The IP address of Certkiller 210.10.20.78 is in the 10.10.20.1 - 10.10.20.255 range. The local interface of the router, 10.10.20.1, should be used as a default gateway.

Incorrect Answers

A: There is no need to create a local user account on a server in order to share resources in the domain.

C: Enabling BOOTP on a router would make sure that DHCP traffic would be forwarded. However, in this scenario the client computer Certkiller 2 has a static address and there is no need for DHCP.

E: The local interface of the router, 10.10.20.1, should be used as a default gateway. 10.10.13.1 is the external interface of the router.

F: The range of IP addresses on the subnet seems to be in the 10.10.20.1 - 10.10.20.255 range. 10.20.30.200 is not in this range.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 8

QUESTION 235

You are the administrator of your company's network. Your network has 200 Windows 2000 Professional computers and 15 Windows 2000 Server computers. Users on the network save their work files in home folders on a network server. The NTFS partition that contains the home folders has Encrypting File System (EFS) enabled.

A user named John leaves the company. You move all of the files from John's home folder to his manager's folder. When the manager attempts to open any of the files, she receives the following error message: "Access denied."

You want the manager to be able to access the files. What should you do?

- A. Grant the manager NTFS Full Control permission to the files.
- B. Grant the manager NTFS Take Ownership permission to the files.
- C. Log on to the network as a Recovery Agent. Decrypt the files for the manager.
- D. Log on to the network as a member of the Backup Operators Group. Decrypt the files for the manager.

Answer: C

Explanation: An encrypted file on an EFS partition can only be decrypted by the owner of file or by the Recovery Agent.

Incorrect Answers:

A: Granting the manager NTFS Full Control permission of the files will not enable the manager to decrypt the files, as an encrypted file can only be decrypted by the owner of file or by the Recovery Agent.

B: Granting the manager NTFS Take Ownership permission of the files will not enable the manager to decrypt the files, as an encrypted file can only be decrypted by the owner of file or by the Recovery Agent.

D: A member of the Backup Operators Group can only restore encrypted files from backup. They cannot decrypt encrypted files. Only the owner of file or a Recovery Agent can decrypt an encrypted file.

Reference:

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 18

QUESTION 236

Your Windows 2000 Professional computer belongs to the contoso.com domain. You need to encrypt a compressed file named C:\data. You successfully encrypt the file but discover that it is no longer compressed.

What is the most likely cause of this problem?

- A. A group policy is preventing the compression of encrypted files.
- B. The file is stored on a FAT32 partition.
- C. Only members of the Administrators and the Power Users groups can compress and encrypt files.
- D. Encrypted files cannot be compressed.

Answer: D

Explanation: A compressed file cannot be encrypted, and an encrypted file cannot be compressed. If you encrypt a compressed file, the file will first be uncompressed and then encrypted. It will no longer be compressed and neither will you be able to compress it once it has been encrypted.

Incorrect answers:

A: There is no Group Policy that prevents compression of encrypted files. A file can either be encrypted or compressed, but not both.

B: The FAT32 file system does not support compression or encryption.

C: Any user with the appropriate file permissions can encrypt and compress files, not just Administrators or Power Users.

Reference:

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 18

QUESTION 237

A user in your company network needs to encrypt a folder that is on her Windows 2000 Professional computer. Her computer has two drives: Drive C and Drive D. The folder that needs to be encrypted is located on Drive D. When the user attempts to encrypt the folder, no option for encryption can be found in the folder properties.

What should you do to enable the user to encrypt the folder?

- A. Log on to her computer as an Administrator, and then run the cipher /e command.
- B. Instruct the user to run the cipher /e command.
- C. Log on to her computer as an Administrator, and then run the Secedit /enforce command.
- D. Instruct the user to run the Secedit /enforce command.
- E. Log on to her computer as an Administrator, and then run the Convert d:/FS:NTFS command.

Answer: E

Explanation: Any ordinary user should be able to encrypt files as long as they have the appropriate permission to the files and the folder, and as long as the file system supports file encryption. The only file system that supports file encryption is the NTFS file system. If this file system is not in use, the option to encrypt files will not be shown. As no option for file encryption can be found, you can assume that the disk uses the FAT or FAT32 file system. This would need to be converted to NTFS to support file encryption. You would need to log on as an administrator and run Convert d:/FS:NTFS at the command prompt, which can be done by clicking on the start button, clicking on Run and then typing cmd in the dialog box. This allows us to convert the drive to the NTFS file system without affecting the data on the drive. However, you cannot convert a drive back to FAT or FAT32.

Incorrect answers:

- A: Any user who has access to a file can encrypt the file. You therefore do not require administrative privileges to encrypt the file and thus you do not need to log on with the Administrator account.
- B: The Cipher /e command would encrypt the files, but only if they were on an NTFS partition.
- C: Secedit is used to apply security templates. The secedit command does not have a /enforce switch.
- D: Secedit is used to apply security templates. The secedit command does not have a /enforce switch.

Reference:

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 18

QUESTION 238

You encrypt your files to ensure the security of the files. You want to make a backup copy of the files and maintain their security settings. You have the option of backing up to either the network or floppy disk.

What should you do?

- A. Copy the files to a network share on an NTFS volume and do nothing further.
- B. Copy the files to a network share on a FAT 32 volume and do nothing further.
- C. Copy the files to a floppy disk that has been formatted by using Windows 2000 Professional.

D. Place the files in an encrypted folder, and then copy the folder to floppy disk.

Answer: A

Explanation: Encryption security settings are retained when an encrypted file is moved or copied to an NTFS volume.

Incorrect answers:

B: The FAT 32 file system does not support file encryption.

C: Floppy disks use the FAT file system, which does not support encryption.

D: Floppy disks use the FAT file system, which does not support encryption.

Reference:

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 18

QUESTION 239

You are the administrator of a Windows 2000 network.

You are configuring eight computers to use both Windows NT Workstation 4.0 and Windows 2000 Professional. Each computer has a 10 GB hard disk. You configure the hard disk on each computer to have two 5 GB partitions. Windows NT Workstation is installed on drive D. Windows 2000 Professional is installed on drive C. In Windows 2000 Professional, you configure a disk quota on drive C to prevent users from saving work files on the disk. You restart the computers and load Windows NT Workstation 4.0. You notice that users can still save files to drive C.

You want to prevent users from saving files to drive C in either operating system. You also want to ensure that users can access both drives while using either operating system.

What should you do on each computer?

A. Reinstall Windows NT Workstation 4.0 after configuring the disk quotas.

B. Use Windows 2000 Professional to configure drive C as a dynamic partition.

C. Use Windows 2000 Professional to enable Encrypting File System (EFS) on drive C.

D. Use Windows NT Workstation 4.0 to configure NTFS permissions on drive C to deny the users Write permission.

Answer: D

Explanation: The Write permission allows you to overwrite the file, change file attributes, and view file ownership and permissions. Thus if you want to allow users access to both drives when using either operating system while preventing them from saving to drive C, then you should deny the write permission to the users as described in option D.

Incorrect answers:

A: This scenario sketches a permissions problem and not a disk quota problem and having to re-install Windows NT Workstation 4.0

B: Configuring Drive C to be a dynamic partition will not prevent users from saving files to drive C.

C: Encryption is not prevention of writing to a drive.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 14, Lesson 1

QUESTION 240

You are the network administrator for Certkiller .

A user needs to encrypt a folder that is on his Windows 2000 Professional computer. His computer has two drives, drive 0 and drive 1. Drive 1 is configured as a dynamic disk with two volumes, D and E. The folder that needs to be encrypted is located on volume E. When the user attempts to encrypt the folder, no option for encryption can be found in the folder properties.

You need to enable the user to encrypt the folder.

What should you do?

- A. Log on to his computer as an Administrator, and then run the cipher /e command.
- B. Log on to his computer as an Administrator, and then run the Secedit /enforce command.
- C. Log on to his computer as an Administrator, and then run the Convert E: /FS:NTFS command.
- D. Log on to his computer using his account, and run the cipher /e command.
- E. Log on to his computer using his account, and run the Secedit /enforce command.
- F. Convert Drive 1 to a basic disk.

Answer: C

Explanation: Any ordinary user should be able to encrypt files as long as they have the appropriate permission to the files and the folder, and as long as the file system supports file encryption. The only file system that supports file encryption is the NTFS file system. If this file system is not in use, the option to encrypt files will not be shown. As no option for file encryption can be found, you can assume that the disk uses the FAT or FAT32 file system. This would need to be converted to NTFS to support file encryption. You would need to log on as an administrator and run Convert d:/FS:NTFS at the command prompt, which can be done by clicking on the start button, clicking on Run and then typing cmd in the dialog box. This allows us to convert the drive to the NTFS file system without affecting the data on the drive. However, you cannot convert a drive back to FAT or FAT32.

Incorrect answers:

A: Any user who has access to a file can encrypt the file. You therefore do not require administrative privileges to encrypt the file and thus you do not need to log on with the Administrator account.

B: Secedit is used to apply security templates. The secedit command does not have a /enforce switch.

D: The Cipher /e command would encrypt the files, but only if they were on an NTFS partition.

E: Secedit is used to apply security templates. The secedit command does not have a /enforce switch.

F: Converting Drive1 to a basic disk will not allow the NTFS file system that is needed if you want the user to be able to encrypt the folder.

Reference:

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 18

QUESTION 241

You upgrade five computers in the Finance organizational unit (OU) from Windows NT Workstation 4.0 to Windows 2000 Professional. The computers are used by members of the Finance OU to run financial Applications. All five computers are configured to have the default security settings.

A user named Helene reports that she can no longer log run the financial applications on her Windows 2000 Professional computer. Prior to the upgrade, Helene was able to run the financial applications on her computer. Helene is a member of the local Users group.

You want the financial applications to run on her computer. What should you do?

A. Use Computer Management to configure separate memory space for each financial application on Helene's computer.

B. Use Security Templates to edit the Security Policy to include the financial application on Helene's computer.

Then add Helene's user account to the Power Users group on Helene's computer.

C. Use Security Configuration and Analysis to reconfigure the default security policy .inf to allow financial applications to run on Helene's computer.

D. Use Secedit.exe to apply the Compatws.inf security template on Helene's Security Policy to loosen the permissions for the local Users group on Helene's computer.

Answer: D

Explanation: The Compatws.inf template relaxes security settings for the Users group and is therefore well suited for workstations that need compatibility with older applications. In fact, the main purpose of the compatws.inf template is to enable non-certified legacy programs to run.

Incorrect answers:

A: Computer Management cannot be used to configure separate memory space for applications.

B: Adding Helene's user account to the Power Users group might make the application run. But it also represents a security risk since ordinary users should not have the rights and permissions of a Power User.

C: It is possible to reconfigure the default security policy to make the application run. This however, demands a lot of administrative effort. It is thus better to use the compatws.inf template, which is designed to allow legacy programs to run.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 13

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 19

QUESTION 242

You upgrade your computer from Windows NT Workstation to a Windows 2000 Professional computer.

070-210

Your computer is a member of the justtalks.com domain. Prior to this upgrade your computer was configured by a system policy to require at least a 12 alphanumeric character password. After the upgrade your computer will not apply the security policy.

What should you do?

- A. Use secedit.exe to refresh the security policy.
- B. Use Local Computer Policy to configure the local security policy.
- C. Use Security Configuration and Analysis to support the security files as a .pol file.
- D. Use Computer Management to configure the security policy setting.

Answer: B

Explanation: In this scenario the Windows NT Workstation 4.0 and Windows 2000 Professional computers have incompatible security settings. The security setting could be correctly configured with a local computer policy. From Control Panel, open the Administrative Tools, open Local Security Policy, select Security Settings, select Account Policies, select Password Policies, and select and Configure Minimum Password Length.

Incorrect answers:

A: The security policy must be correctly configured, not refreshed.

C: Windows 2000 does not use .pol files for security policy settings. .pol files are used on Windows NT computers.

D: Computer Management cannot be used to configure security policy settings; instead the Local Security Policy administrative tool should be used.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 17, Lesson 2

QUESTION 243

You are the administrator of a Windows 2000 network.

You upgrade five computers in the sales department to Windows 2000 Professional. You then apply the Basicwk.inf security template to the upgraded computers. The remaining computers in the sales department are using Windows NT Workstation 4.0. When users log on to the Windows 2000 Professional computers they report that they are unable to run the company's database application. When the users log on to Windows NT Workstation 4.0 computers they are able to run the database application.

You want the users of Windows 2000 Professional computers to be able to run the database application. What should you do?

- A. Apply the Securews.inf security template to the computers.
- B. Apply the Compatsws.inf security template to the computers.
- C. Delete the Basicwk.inf security template file from the computers.
- D. For each user account, grant Read permission to the database application and its associated files.

E. Use the System Policy Editor to configure a new security policy for the database application.

Answer: B

Explanation: The basicwk.inf security template configures the Windows 2000 default security settings. Apparently the database application is a legacy application, which will not run with these default security settings. The compatws.inf template is applied to enable non-certified legacy programs to run successfully under the less secure Power User configuration.

Incorrect answers:

A: The Securews.inf template would put even more restriction on the users. It would not help the users to run the application.

C: By deleting the basicwk.inf the only thing achieved is the possibility of returning to the default security settings are lost. The security settings of the computer are not changed by deleting a security template.

D: By just changing some file permissions you will not enable the database application to run. The users most likely already have read permissions to the application files.

E: The system policy editor was used in downlevel versions of Windows (95, 98, NT) to configure Administrative templates. In Windows 2000 the Group Policy editor is used instead.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 13

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 19

QUESTION 244

You are the network administrator for Certkiller .

A user named Marie uses a Windows 2000 Professional computer named CK1 to process payroll records. You want to prevent CK1 from being able to communicate with any Windows NT Workstation 4.0, Windows 98 and Windows 95 computers on the network. You also want CK1 to communicate only with other Windows 2000 computers.

What should you do?

A. Close all NetBIOS ports in the Advanced TCP/IP options of CK1 .

B. Disable the Access this computer from network policy in the local security policy settings for CK1 .

C. Import the Securews.inf security template to CK1 .

D. Import the Hisecws.inf security template to CK1 .

E. Clear all WINS client settings on CK1 .

Answer: D

Explanation: The Hisecws.inf is the security template that requires the highest level of security and the maximum protection for network traffic and protocols used between computers running Windows 2000. As a

result, computers configured with a highly secure template can only communicate with other Windows 2000 computers. They will not be able to communicate with computers running Windows 95, Windows 98, or Windows NT. The Hisecws.inf security template would increase the security on Marie's computer. However, increasing security would make it harder to connect.

Incorrect Answers:

A: Closing NetBIOS ports will affect Windows 2000 and downlevel Windows clients similarly. In other words it will affect the ability of all other computers to communicate with the computer, thus also hampering communication with other Windows 2000 computers.

B: Disabling the "Access this computer from network" setting would prevent all other computers, including Windows 2000 computers from accessing the computer through the network.

C: The Securews.inf template would put even more restriction on the users. But it would not prevent the users to communicate with CK1 , no matter which type of Windows OS they operate in..

E: Clearing the WINS client settings on Payroll5 will not prevent Windows 95, Windows 98 or Windows NT computers from communicating with Marie's computer, CK1 .

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 13

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 19

QUESTION 245

You use a shared Windows 2000 Professional computer. You notice that some of your Microsoft Word documents that were on the local hard drive have been deleted. You restore the documents from a recent backup.

You want to be able to track all users who access your Word documents in the future. What should you do? (Choose two)

- A. Enable the local group policy for auditing Object Access events that are successful.
- B. Enable the local group policy for auditing Object Access events that are unsuccessful.
- C. Enable the local group policy for auditing Process Tracking events that are successful.
- D. Enable the local group policy for auditing Process Tracking events that are unsuccessful.
- E. Use Windows Explorer to enable auditing for your files.
- F. Run the diskperf -y command. Use System Monitor to examine the logical I/O counter. Restart the computer.

Answer: A, E

Explanation: Auditing is a two-step process. First you must enable the auditing on the right kind of object; in this scenario you would want to audit 'Object Access'. This includes files, folders and printers. You must also decide if you are going to audit success or failure, or both success and failure. In this scenario you will use success since you want to audit access of the Word documents. Then you must use Windows Explorer to enable the auditing on specific resources. In this scenario it is the files and folders that should be audited.

Incorrect answers:

B: You must track successful object access, not unsuccessful, since you want to track the access of the Word documents.

C: To track access to Word documents you must use audit Object Access and not Process Tracking.

D: To track access to Word documents you must use audit Object Access and not Process Tracking.

F: The diskperf -y switch was used in Windows NT 4.0 to enable physical disk performance counters. These counters are enabled by default in Windows 2000. Furthermore, performance counters cannot be used to audit network access.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 16, Lesson 3

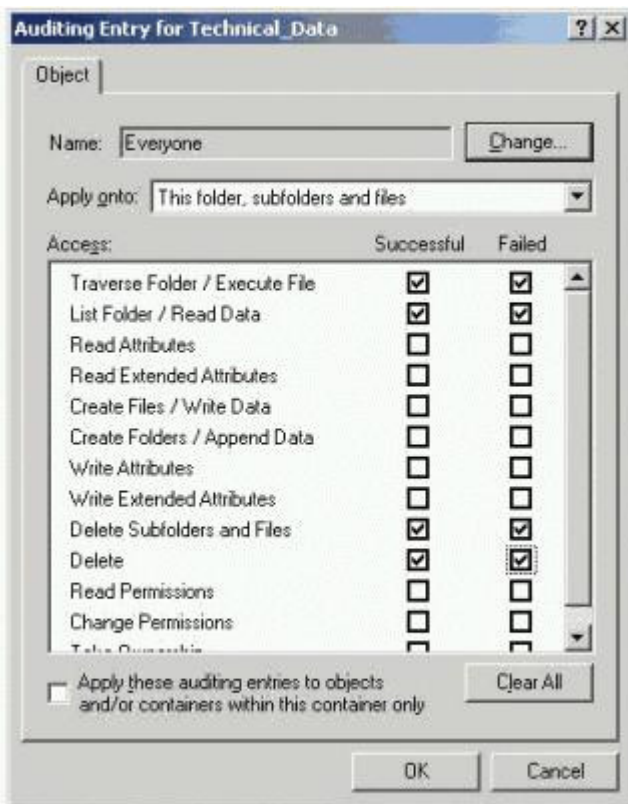
Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 20

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 13

QUESTION 246

You are the administrator of a Windows 2000 network. A user named Carlos configures a shared folder named Technical_Data on his Windows 2000 Professional computer. Carlos wants to audit access to the Technical_Data folder and track any attempts to delete files.

Carlos configures auditing for Technical_Data, as shown in the exhibit.



The Security Log on Carlos's computer is set to a maximum log file size of 512 KB and to overwrite events as needed.

The next day Carlos reports that files were deleted from the Folder. However, no events were generated

in his computer's Security Log.

Carlos needs to discover who is deleting files on his computer. What should you do?

- A. Restart the Security Accounts Manager Service.
- B. Modify the Security Log size settings to set the file size to 2,048 KB.
- C. In the Local Security Policy setting for Audit Object Access, select the Success and Failure check boxes.
- D. In the Auditing Entry dial box for Technical_Data, select the Change button and change Everyone to Authenticated Users.

Answer: C

Explanation: Enabling auditing is a two-step procedure. First we define an Audit Policy and then we configure the objects that we want to audit. In this scenario we should Audit Object Access for Success and Failure.

Incorrect Answers

A: There is no reason to restart the Security Accounts Manager Service.

B: The Security log is empty. The maximum size of it is not a problem.

D: The Everyone group includes all Authenticated Users. This would only restrict auditing somewhat.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 16, Lesson 3

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 20

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 13

QUESTION 247

You are the network administrator for Certkiller and you support the portable computer users. An Account Executive named Hildegard frequently travels to meet with customers and uses her portable computer to demonstrate the company's new software products. Hildegard needs to update these products frequently so customers can evaluate the latest software releases.

You need to allow Hildegard to install the product updates while limiting her ability to perform other administrative duties on her portable computer.

What should you do?

- A. Add Hildegard's user accounts to the Pre-Windows 2000 Compatible Access group.
- B. Add Hildegard's user account to the local Power Users group.
- C. Allow Hildegard's user account Full Control permission to the Program Files folder. Propagate the permissions to all the subdirectories and files in that directory.
- D. Allow Hildegard's user account Write permissions to the Program Files folder. Propagate the permissions to all the subdirectories and files in that directory.

Answer: B

Explanation: As a member of the local Power Users group, Hildegard would be able to install and update applications.

Incorrect Answers

A: By default, the Everyone special group is already a member of the Pre-Windows 2000 Compatible Access group. So Hildegard is already a member of this group. Furthermore, membership of this group does not affect the rights or permissions to install applications.

C, D: Permissions to the Program Files folder has no particular significance.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 11, Lesson 2

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 7

QUESTION 248

You are the network administrator for Certkiller Inc. Two users named Eric and Julia share a Windows 2000 Professional computer. Eric's user account is a member of the local Administrators group. Eric needs to share files with Julia. Eric wants Julia to be able to change any of the shared files and to create her own files if necessary. Eric wants to prevent Julia from changing the permissions on files that Eric creates.

To accomplish his goal, Eric creates a folder named C:\Data. He changes the NTFS permission on C:\Data to allow his local user account Full Control permissions and to allow Julia's local user account default permissions. Eric places 10 files in the folder.

When Julia logs on to the computer using her local user account and opens a file in C:\Data, she cannot save the changes to the file. Julia also cannot create any new files in the folder.

You need to help Eric configure the correct permissions of C:\Data. What should you instruct Eric to do?

- A. Add Julia's user account to the local Power Users group.
- B. Add Julia's user account to the local Administrators group.
- C. Allow Julia's user account Write permissions to C:\Data.
- D. Allow Julia's user account Full Control permission to C:\Data.

Answer: C

Explanation: Write permissions would allow Julia to save changes to files and create new files as is required. Furthermore, she would not be able to change any file permissions.

Incorrect Answers

A: The Local Power Users group would not have any additional permissions to the folder. Julia would not be able to perform the required tasks.

B: As a member of the local Administrators group, Julia would be able to do whatever she wants with the files, including changing permission on the files Eric creates.

D: Full Control permissions would enable Julia to change permissions on Eric's files.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 11, Lesson 2

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 7

QUESTION 249

You are a system administrator at Certkiller . The network includes 100 Windows 2000 Professional computers. A user named Peter wants to share a local printing device directly connected to his computer. Peter needs to share this device among three groups: Engineering, Accounting, and Operations. Peter wants to delegate printer administration to one print administrator from each group. Each print administrator must be able to delete print jobs generated by their own group on the print device. They should not be able to delete print jobs from other groups. You want to configure Peter's client computer to support these requirements. What should you do?

- A. Create a single shared printer to be used by all three groups. Allow each print administrator Manage Documents permission.
- B. Create a separate shared printer for each group. For each shared printer, allow the respective print administrator Manage Documents permission.
- C. Create a single shared printer to be used by all three groups. Add the print administrator's user account from each group to the Power Users group on Peter's client computer.
- D. Create a separate shared printer for each group. Add the print administrator's user account from each group to the Power Users group on Peter's client computer.

Answer: B

Explanation: We need a printer for each group. We then only grant Manage Document permission to the single appropriate printer for each print administrator.

Incorrect Answers

A, C: A single printer would enable the print administrators to manage all print jobs, including print jobs from other groups.

D: As a member of the Power Users group have the Manage Printers permission for all printers, they would be able to manage print jobs from other groups.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 11, Lesson 2

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 7

QUESTION 250

You are the administrator of a Windows 2000 network. You need to store secured files for your company's Accounting and Legal departments on a Windows 2000 Professional computer.

You want to accomplish the following goals:

- Enable users in both departments to access their own files from the network
- Enable users in the Accounting department to view the Legal department's documents
- Prevent users in the Legal department from being able to view the Accounting department's documents
- Enable managers within the company to access and modify both the Accounting and the Legal department's files

You take the following actions:

- Create two shared folders named Accounting and Legal
- Create three groups named Accounting, Legal, and Management
- Allow the Accounting group Modify permission on the Accounting folder
- Allow the Accounting group Read permissions on the Legal folders.
- Allow the Management group Modify permission on both the Accounting and Legal folders.

Which result or results do these actions produce? (Choose all that apply)

- A. Users in both departments can access to their own files from the network.
- B. Users in the Accounting department can view the Legal department's documents.
- C. Users in the Legal department cannot view the Accounting department's documents.
- D. Company managers can access and modify both departments' files.

Answer: B, C, D

Explanation:

B: The Accounting group has been granted Read permission to the Legal folders so they can view the Legal department's documents.

C: The Legal group has not been granted any permissions so they cannot access the Accounting department's documents.

D: The Company Management's group has Modify permissions to both the Accounting and the Legal folders so they will be able to modify both departments' files.

Incorrect Answers

A: The Accounting group can access the Accounting folder, but the Legal group has not been granted any permission so they cannot access their own files.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 11, Lesson 2

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 7

QUESTION 251

You are the administrator of a Windows 2000 Professional computer. A user named Maria assists you in

070-210

performing some administrative tasks. Maria is a member of local Administrators group.

Users report that Maria has been viewing and changing their files. You want Maria to be able to install programs, perform backups and manage printers, but not to view, change or read other users' files for which permission has not been granted.

You want to set up Maria's account to have minimal rights and permission. You want to accomplish this with least amount of administrative effort.

What should you do?

A. Leave Maria in the local Administrators group.

Limit her rights by using Local Policies.

B. Leave Maria in the local Administrators group.

Change the NTFS provision on other users' files to deny Maria's request.

C. Remove Maria from the local Administrators group.

Add her to both the Power Users group and Backup Operators group.

D. Remove Maria from local Administrators group.

Add her to Power User group.

Then grant her NTFS Read permission on the files to be backed up.

Answer: C

Explanation: By adding Maria's user account to the Power Users group Maria will inherit the ability to share resources and install programs that is conferred on members of the Power Users group. To grant Maria the ability to backup files she must be added to the Backup Operators group, which has the permissions to backup files. As a member of this group Maria will be able to backup files as she will inherit those rights by virtue of being a member of that group. Maria will not have permissions to read the users' files as she has been removed from the local administrators group and as neither the Power Users group nor the Backup Operators group has the permissions to read other users' files.

Incorrect Answers:

A: Leaving Maria in the local Administrators group would allow her to view, read and change the files of the users. As the local administrators group enjoy these permissions.

B: Leaving Maria in the local Administrators group would allow her to take ownership of any file and then view, read or change it as the local Administrators group enjoys this permission.

D: Giving Maria read permission on the files she must backup would be against the wishes of the users; they do not want Maria to be able to view their files.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 11, Lesson 2

QUESTION 252

You are the network administrator for Certkiller .

There are 200 Windows 2000 Professional computers on your network. All computers on the network access the Internet by using a Microsoft Proxy Server computer named Proxy1. The IP address of Proxy1 is 192.168.99.5. You discover that Proxy1 is experiencing performance degradation due to the large

number of requests to authenticate with the proxy server.

You want to minimize the number of authentication requests to the proxy server.

What LAN configuration should you modify on each computer?

To answer, select the appropriate configuration setting or settings that should be modified in the Local Area Network Settings dialog box in the Work Area.

Possible Addresses

192.168.99.5
192.168.99.5

Possible Ports

80
443

Work Area

Answer:

QUESTION 253

You are the network administrator for Certkiller .

Certkiller 's Account Executives frequently travel to meet with customers. The Account Executives use their portable computers to demonstrate Certkiller 's new software products. The Account Executives need to update these products frequently so customers can evaluate the latest software releases. The Account Executives also need to be able to change display settings on their portable computers. You need to allow the Account Executives the ability to install and update software products while limiting their ability to perform other administrative duties on their portable computers. You need to accomplish this with the least amount of administrative effort.

What should you do?

- A. Add the Account Executive's user accounts to the local Administrators group on their portable computers.
- B. Add the Account Executive's user accounts to the Pre-Windows 2000 Compatible Access group.
- C. Add the Account Executive's user accounts to the local Power Users group on their portable computers.
- D. Allow the Account Executive's user accounts Full Control permission to the Program Files folder on their portable computers. Propagate the permissions to all the subdirectories and files in that directory.

Answer: C

Explanation: The Power Users group is a built-in group. By default, the group has no members. Power Users can create local users and groups; modify and delete accounts that they have created; and remove users from the Power Users, Users, and Guests groups. Power Users also can install most applications; create, manage, and delete local printers; and create and delete file shares.

Incorrect Answers:

A: We need to limit the Account Executive's ability to perform administrative duties on their portable computers. Therefore, they should not be added to the local Administrators group.

B: The Pre-Windows 2000 Compatible Access group allows an NT RAS server to authenticate a remote access user in a Windows 2000 domain. This group cannot be used in this scenario.

D: Granting Full Control permission to the Program Files folder won't enable the users to install applications. This is because applications also need to write information to the registry, which the users won't have permission to do.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 7

QUESTION 254

You are the network administrator for Certkiller .

You are responsible for creating and deploying a standard Windows 2000 Professional image to 1,000 client computers, You log on to a client computer named Computer1 by using a local administrator account named User1. On Computer1, you install three software packages that are compatible with Windows 2000 Professional.

You create an image using third-party software. You deploy the image to a test client computer and join that computer to a domain. When you log on to the test client computer with a domain user account, the new applications do not appear in the Start menu.

You want to re-create the image to include the applications in the Start menu for all new users. You also want to allow the users to delete any icons they do not need.

Which profile should you copy?

To answer, select the correct profile from the Source Profile area and drag it to the correct field in the Target Profile area.



Answer:

QUESTION 255

You are the administrator of your company's network. Ten Windows 2000 Professional computers are located in the Research department. The computers contain highly confidential information.

You want the 10 computers to be able to communicate with other Windows 2000 Professional computers on the network. However, you do not want them to communicate with computers that are not running Windows 2000, including those that are running Windows 95, Windows 98 and Windows NT.

You want to configure a security policy on each computer to ensure that the confidential information is secure. What should you do?

- A. Use Security Configuration and Analysis to import the Hisecws.inf security template file to modify the default security settings.
- B. Use security templates to create a security template file and import the security settings to modify the default security settings.
- C. Use the local computer policy to disable the access to this computer from the network option.
- D. Use Secedit.exe to reconfigure the computers' default security settings to not allow anonymous access to the computers.

Answer: A

Explanation: The Hisecws.inf, the highly secure template, is used to require maximum protection for network traffic and protocols used between computers running Windows 2000. As a result, such computers configured with a highly secure template can only communicate with other Windows 2000 computers. They will not be able to communicate with computers running Windows 95, Windows 98, or Windows NT.

Incorrect answers:

B: It is possible to make the appropriate changes to the security template manually but this is a daunting administrative task. It would be easier to use a predefined security template.

C: The Windows 2000 computers must be able to access each other. You therefore cannot disconnect the local computer from the network.

D: Anonymous access is not handled by the security settings. It is handled by enabling or disabling the Guest account, and by giving or restricting permissions to the Everyone group.

Disabling anonymous access, by disabling the Guest account and removing permissions from the Everyone group, would not differentiate between Windows 2000 computers and downlevel Windows systems.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 13

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 19

QUESTION 256

You want to prevent a Windows 2000 Professional computer named Payroll5 from communicating on your network with Windows NT 4.0, Windows 95, and Windows 98 computers. You want to enable the

Payroll5 computer to communicate on your network with other Windows 2000 computers only. What should you do?

- A. Close all NetBIOS ports in the Advanced TCP/IP options of Payroll5.
- B. Import the Hisecws.inf security template to Payroll5.
- C. Disable Access this computer from network in the local security policy settings for Payroll5.
- D. Clear all WINS client settings on Payroll5.

Answer: B

Explanation: The Hisecws.inf is the security template that requires the highest level of security and the maximum protection for network traffic and protocols used between computers running Windows 2000. As a result, computers configured with a highly secure template can only communicate with other Windows 2000 computers. They will not be able to communicate with computers running Windows 95, Windows 98, or Windows NT.

Incorrect Answers:

A: Closing NetBIOS ports will affect Windows 2000 and downlevel Windows clients similarly. In other words it will affect the ability of all other computers to communicate with the computer.

C: Disabling the "Access this computer from network" setting would prevent all other computers, including Windows 2000 computers from accessing the computer through the network.

D: Clearing the WINS client settings on Payroll5 will not prevent Windows 95, Windows 98 or Windows NT computers from communicating with Payroll5.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 13

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 19

QUESTION 257

You are the administrator of a Windows 2000 Professional computer. The computer is a member of a Windows 2000 domain. The domain contains an enterprise certification authority (CA). You use the computer to connect to the Internet.

Six months ago, you paid for online computer support services from a support company. The support company's Web site is at <https://www.Certkiller.com>. Now you attempt to connect to the Web site again to use the support service. Before the Web page is displayed, you receive a dialog box. The message in the dialog box asks you to select a certificate to use when you connect. However the list of certificates that is shown in the dialog box is empty. You cannot select a certificate and you cannot connect to the company's Web page.

In Internet Explorer, you open the Internet Options dialog box and check Certificates. Several personal certificates appear in the Advanced Purposes list.

You want to be able to connect to the support company's Web site at <https://www.Certkiller.com>. What should you do?

070-210

- A. Configure Internet Explorer to enable the Use TLS 1.0 option.
- B. Add the server certificate for www. Certkiller s.com to the Trusted Publishers list.
- C. Contact the support company to obtain a certificate and add the certificate to the list of personal certificates.
- D. Request a user certificate from the enterprise CA.
- E. Change the security settings of the Internet zone to enable the Anonymous logon option.

Answer: C

Explanation: Secure Sockets Layer (SSL) uses certificates for authentication. Thus we need to provide a valid certificate to be able to access the support site. We should ask the support company to provide us with an appropriate certificate.

Incorrect Answers

- A: TLS (Transport Layer Security) 1.0 is used for backward compatibility. It would not be helpful here.
- B: The scenario does not seem to indicate that the client receives any server certificate from the support company. The client is immediately required to provide a certificate.
- D: A certificate from a local Certificate Authority would no help accessing the external site.
- E: Logon credentials are not used with SSL. Certificates are used instead.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 13

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part II, Chapter 13

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional, Microsoft Press, Redmond, 2000, Chapter 18, Lesson 3

QUESTION 258

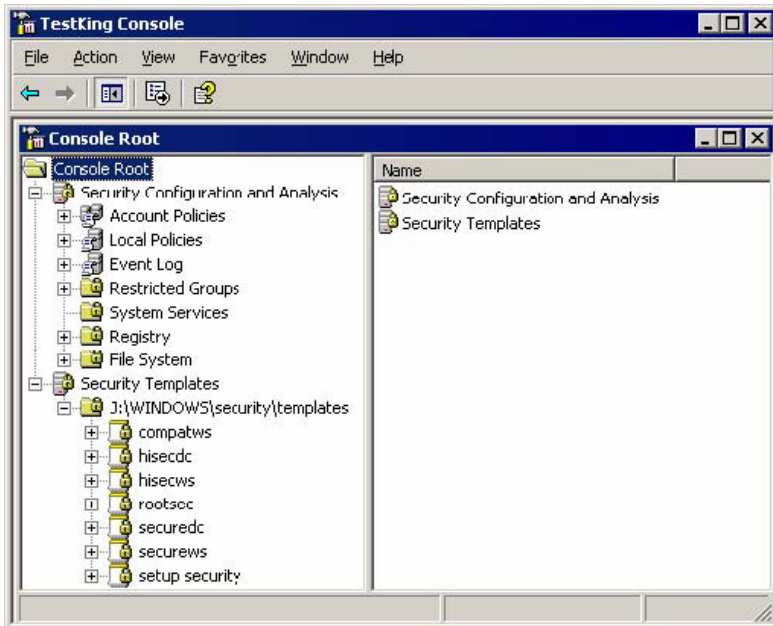
You are the desktop administrator for Certkiller Inc. The company's network contains 500 Windows 2000 Professional computers.

The information security department releases new security requirements. The new requirements state that the Telnet service may not be started on any company-owned client computer.

You need to create a new security template that prevents the Telnet service from starting on companyowned client computers. You open the Security Configuration and Analysis console on your Windows 2000 Professional computer.

Which portion of the console do you need to configure?

To answer, click the appropriate container in the Security Configuration and Analysis console.



Answer: System Services

Explanation: System Services under the Security Configuration and Analysis tab, facilitates the disabling of Telnet service. First we select System Services and then double-click on Telnet. Then we disable the Telnet service.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 13

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 19

QUESTION 259

You are the network administrator for Certkiller .

A user named Marie uses a Windows 2000 Professional computer named Client1 to process payroll records. Marie reports that she can no longer run her financial applications. You determine that file permissions have been applied incorrectly to her computer.

You want to configure Client1 to have the same security configuration and file permission settings that were applied when the computer was installed.

What should you do?

- A. Grant users Full Control permission to the C drive and all child folders.
- B. Use the Recovery Console to restore system files.
- C. Use Security Configuration and Analysis to apply the Secure security template to Client1.
- D. Use Security Configuration and Analysis to apply the Default security template to Client 1.

Answer: D

Explanation: Security Configuration and Analysis offers the ability to compare the security settings of a computer to a standard template, view the results, and resolve any discrepancies revealed by the analysis. You can also import a security template into a Group Policy object and apply that security profile to your computer or to many computers at once. If Client1 is to have the same security configuration and file permission settings that were applied when the computer was installed, then you should make use of Security Configuration and Analysis to apply the default security template to Client1.

Incorrect answers:

A: This option is not the solution. Full control being granted means that you will be able to apply many permissions, etc., but it is not necessary to grant those permissions when you need to just use the Security Configuration and Analysis to apply the Default security template.

B: There is no need to recover system files, as the question states that you want Client1 to have the same file permission settings and security configuration that was applied at installation.

C: You should apply the Default security template and not the Secure security template to Client1.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 13

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 19

QUESTION 260

You are the network administrator for Certkiller .

Computers on your network run Windows 2000 Professional, Windows NT Workstation 4.0 and Windows 98. Ten Windows 2000 Professional computers are located in the research department. These computers contain highly confidential information.

You want the 10 Windows 2000 Professional computers to be able to communicate only with other Windows 2000 computers.

What should you do?

A. On the research computers use the Local Computer Policy to disable the Access this computer from the network option.

B. Use Security Configuration and Analysis to apply the Highly Secure security template to the research computers.

C. Add the users of the research computers to the Power Users group on each computer.

D. On the research computers configure the security settings to prevent anonymous access.

Answer: B

Explanation: Security Configuration and Analysis offers the ability to compare the security settings of a computer to a standard template, view the results, and resolve any discrepancies revealed by the analysis. You

can also import a security template into a Group Policy object and apply that security profile to your computer or to many computers at once. Windows 2000 contains several predefined security templates appropriate to various levels of security and to different types of clients.

The Hisecws.inf is the security template that requires the highest level of security and the maximum protection for network traffic and protocols used between computers running Windows 2000. As a result, computers configured with a highly secure template can only communicate with other Windows 2000 computers. They will not be able to communicate with computers running Windows 95, Windows 98, or Windows NT.

Incorrect answers:

A: If you want the Windows 2000 Professional computers to communicate only with the other Windows 2000 computers, then you should make use of the Security Configuration and Analysis to apply Highly Secure security template and not disable the Access this computer from the network option. This option will not ensure communication with only Windows 2000 Professional computers.

C: Adding the Research computers to the Power Users group is not going to ensure that they communicate only with the other Windows 2000 Professional computers.

D: Configuring the research computers' security settings to prevent anonymous access is not the same as restricting communication to only Windows 2000 Professional computers.

Reference:

Martin Holladay, Microsoft Windows 2000 Professional Resource Kit, Microsoft Press, Redmond, 2000, Part III, Chapter 13

Ed Bott & Carl Siechert, Microsoft Windows Security for Windows XP and Windows 2000 Inside Out, Microsoft Press, Redmond, 2003, Part IV, Chapter 19

QUESTION 261

You are administering a Windows 2000 network at Certkiller .com.

You are configuring your computer to use both Windows 2000 Professional and Windows 98. Your computer has three 8 GB hard disks: Disk 0, Disk 1, and Disk 2. You want to configure each hard disk to have an 8 GB partition. You want to install Windows 98 on Disk 0 and Windows 2000 Professional on Disk 1. You want to store your work files on Disk 2. You want to implement file level security on Disk 1. You want to be able to access your work file when using either operating system.

What should you do?

To answer, drag the correct file system from the File System Type area and drop the file system into the

appropriate Partition type for each hard disk.

Drag and Drop

Disk 0

Disk 1

Disk 2

Partition type	Partition type	Partition type
----------------	----------------	----------------

File System Type. Select from these

Format as FAT	Format as FAT32	Format as NTFS
---------------	-----------------	----------------

Answer:

Disk 0

Disk 1

Disk 2

Format as FAT32	Format as NTFS	Format as FAT32
-----------------	----------------	-----------------

File System Type. Select from these

Format as FAT	Format as FAT32	Format as NTFS
---------------	-----------------	----------------

QUESTION 262

Exhibit



You are administering a Windows 2000 network at Certkiller .com.

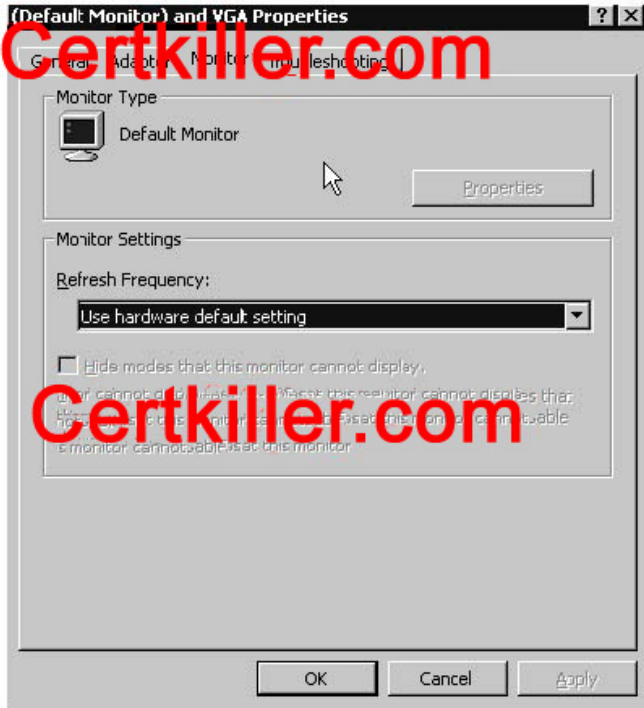
- A. Use Add/Remove Hardware in Control Panel to update the drivers for the device.
- B. Use Device Manager to enable the device.
- C. Move the video capture card to a different PCI slot.
- D. Uninstall the device and disable plug and play detection for the device

Answer: A

Explanation: Windows has detected the device (the device with the '?' in the exhibit), but the correct device driver has not been installed. The Add/Remove Hardware wizard can be used to install the correct device driver.

QUESTION 263

Exhibit:



You are a desktop administrator for Certkiller .com.

You install Windows 2000 Professional on a computer that has a non Plug and Play video adapter. You want to configure the video adapter to use 24 bit color and 800 x 600 resolution. The color setting for the video adapter is set to 16 colors, and you cannot change that setting.

The video adapter properties are shown in the (Default Monitor) and VGA Properties dialog box in the exhibit.

You want to be able to change the color setting for the video adapter.

What should you do?

- A. Use List All Modes to select the adapter default mode.
- B. Change the adapter refresh rate to 60 MHz.
- C. Update the monitor drivers to WDM compliant drivers.
- D. Change the screen resolution to be 1024 x 768.

Answer: C

QUESTION 264

You are the network administrator for Certkiller .com.

You have implemented the Hisecws.inf security template on all the Windows 2000 Professional computers in your network by using a GPO. A user has received a driver and utility software for the internal SCSI controller on his computer. The SCSI controller is not currently on the HCL. He uses the manufacturer provided CD to install the driver and the utility. He restarts the computer and reports that the internal SCSI controller is not working correctly.

You want to allow all users to install this driver on their client computers. You want to accomplish this task with the least amount of administrative effort.

What should you do?

- A. Modify the GPO to change the Driver Signing option.
- B. Run the Sigverif command on each client computer.
- C. Reconfigure the Driver Signing option on each client computer. Install the driver on each client computer. Reapply the security template settings on each client computer.
- D. Modify the Hisecws.inf security template on each client computer to change the Driver Signing option.
- E. Modify the Hisecws.inf security template on the domain controller to change the Driver Signing option.

Answer: A

QUESTION 265

You are the network administrator for Certkiller .com.

You install Windows 2000 Professional on your portable computer. You use a docking station for your portable computer when you are in the office. You install a ISA-based network adapter in your docking station. You insert your computer into the docking station and start the computer. The network adapter is not detected during the startup process. You obtain a disk that contains the supported driver from the network adapter manufacturer.

You want to allow Windows 2000 Professional to use the network adapter.

What should you do? (Each correct answer presents part of the solution. Choose two.)

- A. Restart the computer in the docking station.
- B. Run the Add/Remove Hardware wizard.
- C. Use Device Manager to scan for hardware changes.
- D. Copy the network adapter driver to the Winnt\Driver Cache\i386 folder.
- E. Install the new network adapter driver.

Answer: B, E

QUESTION 266

You are administering a Windows 2000 network at Certkiller .com.

A user named Sandra has a Windows 2000 Professional computer with two physical hard disks. Each hard disk has a single partition. Sandra reports that applications on her Windows 2000 Professional computer are running slowly. You notice that Sandra's computer has 64 MB of RAM. Disk C contains 70 MB of free disk space and Disk D contains 160 MB of free disk space.

You want to improve the performance of Sandra's computer.

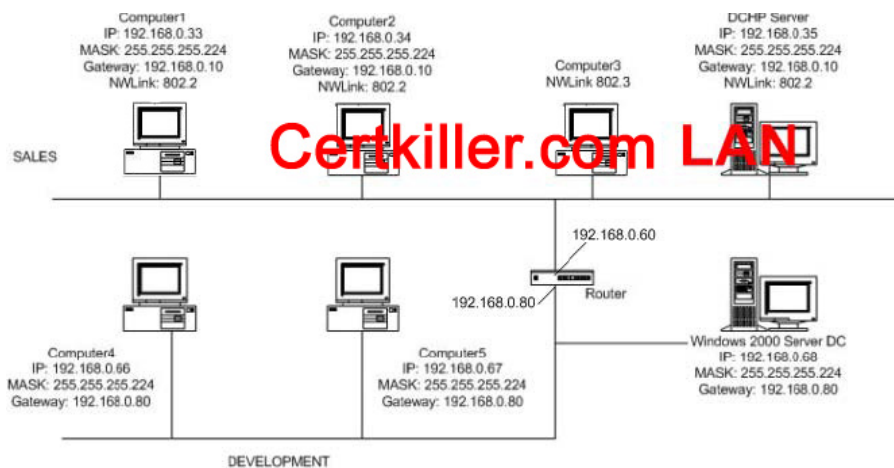
What should you do? Select all that apply.

- A. Delete the paging file.
- B. Set the total paging file to 50 percent of physical memory.
- C. Perform a disk analysis, and use the disk defragmenter if recommended.
- D. Ensure that the Performance Options windows is optimized for applications.
- E. Ensure that the Performance Options windows is optimized for background services.

Answer: C, D

QUESTION 267

You are the administrator of a Windows 2000 network at Certkiller .com. The network is configured as shown in the exhibit.



Computers on the Sales subnet run Windows 2000 Professional. These computers are dynamically assigned IP addressing and configuration information from a DHCP server on the subnet.

Computers on the development subnet run Windows 98. These computers are statically assigned IP addressing and configuration information.

070-210

Users on the Sales subnet report that they cannot communicate with users on the development subnet. A user who works on computer3 reports that he cannot communicate with computers on either subnet. You want all users to be able to communicate with other users on both subnets.

What should you do? (Choose two)

- A. Enable TCP/IP protocol with the default settings on Computer3.
- B. Change the frame type to 802.2 on computer3.
- C. Enable NetBEUI protocol on all computers on both subnets.
- D. Change the default gateway DHCP scope option to 192.168.0.60
- E. Change the default gateway DHCP scope option to 192.168.0.80

Answer: A, D

Explanation: The computers on the Sales subnet cannot communicate with any computers on the development subnet, but they communicate with each other with the exception of computer3, which cannot communicate at all. An incorrect default gateway address on the computers within the Sales subnet explains why they cannot communicate with the development subnet. This problem is resolved by changing the default gateway option on the DHCP server. It is set to IP address of the local Sales interface of the router..

Computer3 also needs to be configured with the TCP/IP protocol to be able to communicate with the other computers.

Incorrect answers:

B: Changing the frame type to 802.2 on computer3 would allow computer3 to communicate with the other computers on the Sales subnet, but it would not allow communication with the computers on the development subnet which all use TCP/IP.

C: NetBEUI is not a routable protocol. It would not allow communication between any of the subnets.

E: The Router interface in the Sales network has the IP address of 192.168.0.60, not 192.168.0.80.

Reference:

Rick Wallace, Self-Paced MCSE Training Kit (Exam 70-210)-Microsoft Windows 2000 Professional,
Microsoft Press, Redmond, 2000, Chapter 8, Lessons 1 & 2