

70-291 Managing Windows Server 2003 Network Infrastructure

1

You are a network administrator for Alpine Ski House. The network consists of a single Active Directory domain named `alpineskihouse.com`.

Your company acquires a company named Adventure Works. The Adventure Works network consists of a single Active Directory domain named `adventure-works.com`.

A server named Server32 is a network-management application server in the `adventure-works.com` domain. Server32 accesses all of the desktop client computers to perform automated software upgrades and hardware inventory. The network-management software on Server32 references desktop computers by unqualified host names, which are resolved to `clientname.adventure-works.com` by using a DNS server.

You join Server32 to your domain to become `server32.alpineskihouse.com`. The Server32 IP address is `10.10.10.90`.

You are gradually migrating all `adventure-works.com` desktop client computers to your domain to become `clientname.alpineskihouse.com`. You do not have access to the `adventure-works.com` DNS server. When Server32 attempts to apply an update to the client computers, the network-management software returns many alerts that say that desktop computers cannot be found.

You want to allow the network-management software on Server32 to resolve unqualified client computer host names in `adventure-works.com` or `alpineskihouse.com`, and you want to use the minimum amount of administrative effort.

What should you do?

- A. On the DNS server for `alpineskihouse.com`, add a zone for `adventure-works.com`. Create a host (A) record for `server32.adventure-works.com` that points to `10.10.10.90`.
- B. On Server32, in **System Properties**, type **adventure-works.com** in the **Primary DNS suffix of this computer** field in the **DNS Suffix and Netbios Computer Name** setting.
- C. On Server32, configure a Hosts file that contains the name and IP address of every network computer.
- D. On Server32, in **Advanced TCP/IP Settings**, add `adventure-works.com` and `alpineskihouse.com` to the **Append these DNS suffixes (in order)** setting.

2

You are the network administrator for your company. The Denver office is currently connected to the corporate WAN by using a Windows Server 2003 computer named Server23.

Server23 is configured as a dial-up router. Server23 has two network adapters. One network adapter connects to the Ethernet LAN. The other network adapter is a broadband networking device.

The company plans to increase the number of employees in the Denver office by at least 25 percent. You need to confirm that the current network bandwidth of the broadband connection will be sufficient for the future expansion of the Denver office.

You want to use System Monitor on Server23 to find out the current utilization of the broadband network connection.

What should you do?

- A. Monitor the Bytes Total/sec counter on the Network Interface object.
- B. Monitor the Bytes Total/sec counter on the Server object.
- C. Monitor the Server\ \Packets/sec counter on the Server object.
- D. Monitor the Current Bandwidth counter on the Network Interface object.

3

You are the administrator of an Active Directory domain. All servers run Windows Server 2003.

You configure a server named Server3 as the DNS server for the domain.

The company recently started using a new ISP. Since the change to the new ISP occurred, users report that they cannot access Internet Web sites by using their fully qualified domain names (FQDNs).

You manually configure a test computer to use the DNS server address of the new ISP. The test computer can successfully access Internet Web sites by using their FQDNs.

You need to ensure that network users can access Internet Web sites by using their FQDNs, while ensuring that user access to internal resources is not disrupted.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

- A. Create a root zone on Server3.
- B. Configure Server3 to use the default root hints.
- C. Configure a forwarder on Server3 to the new ISP's DNS server.
- D. Configure all computers on your network to use the new ISP's DNS server.

4

You are the network administrator for your company. All servers run Windows Server 2003. All servers are configured with static IP addresses. All client computers run Windows XP Professional. All client computers are configured as DHCP clients.

The company has a main office and one branch office. The offices are separated by a router. A DHCP server is deployed in each office. The DHCP servers are named DHCP1 and DHCP2.

You configure scopes on the DHCP1 and DHCP2 as shown in the following table.

DHCP server name	Scope name	Scope addresses
DHCP1	Main	10.1.16.0 - 10.1.31.254
DHCP1	Branch	10.2.28.0 - 10.2.31.254
DHCP2	Main	10.1.28.0 - 10.1.31.254
DHCP2	Branch	10.2.16.0 - 10.2.31.254

You shut down DHCP1 for scheduled maintenance. While DHCP1 is shut down, client computers in both offices continue to receive correct IP address assignments from DHCP2.

You restart DHCP1. Several users report that when they restart their computers, they receive error messages stating that a duplicate IP address exists on the network.

You need to ensure that these error messages do not appear when you shut down and restart a DHCP server. You need to ensure that changes you make does not affect the current DHCP functionality.

What should you do?

- A. On each DHCP server, configure a superscope that includes both DHCP scopes.
- B. Configure the router between the offices to block all broadcasts.
- C. Modify the Main scope on DHCP1 to include addresses 10.1.16.0 through 10.1.27.254. Modify the Branch scope on DHCP2 to include addresses 10.2.16.0 through 10.2.27.254.
- D. Modify the Main scope on DHCP2 to include addresses 10.1.16.0 through 10.1.31.254. Modify the Branch scope on DHCP1 to include addresses 10.2.16.0 through 10.2.31.254.

5

You are the administrator of a Windows Server 2003 computer named Server1. Server1 has a third-party application installed on it. The third-party application runs as a service that is named Service1. Service1 fails periodically.

You need to configure the recovery options for Service1 to meet the following requirements:

- If Service1 runs successfully for a day or more, you need to ensure that only the service is immediately restarted upon failure.
- If, after this failure, Service1 does not run successfully for another day, you must ensure the entire server is immediately restarted.

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

- A. Configure the **Reset fail count after** value for Service1 to 1 day.
- B. Configure the **Restart service after** value for Service1 to 1,440 minutes.
- C. Configure the response to the first failure to be to restart Service1.
- D. Configure the response to the first failure to be to restart Server1.
- E. Configure the response to the second failure to be to restart Service1.
- F. Configure the response to the second failure to be to restart Server1.

6

You are the network administrator for your company. The network consists of a single Active Directory domain. The domain contains Windows Server 2003 computers and Windows XP Professional computers.

You configure a server named Server1 to be a file server. The written company security policy states that you must analyze network traffic that is sent to and from all file servers.

You need to capture file-transfer network traffic that is being sent to and from Server1. You install Network Monitor Tools from a Windows Server 2003 product CD-ROM on a server named Server2, which is on the same network segment as Server1.

You run Network Monitor on Server2. However, Network Monitor captures only network traffic that is sent to and from Server2. You need to capture all network traffic that is sent to and from Server1.

What should you do?

- A. Install the Network Monitor driver on Server1. Run Network Monitor on Server2 to capture network traffic.
- B. Open Network Monitor on Server2 and create a capture filter to enable the capture of all protocols. Run Network Monitor to capture network traffic.
- C. Install Network Monitor Tools on Server1. Run Network Monitor to capture network traffic.
- D. Open Network Monitor on Server2 and increase the capture buffer from 1 MB to 20 MB in size. Run Network Monitor to capture network traffic.

7

You are the network administrator of your company. The company network contains two subnets that are connected by a router. All servers run Windows Server 2003.

All network hosts are manually configured with TCP/IP information. The network is configured as shown in the exhibit. (Click the **Exhibit** button.)

A developer uses a server named Workstation6 for testing. She reports that she cannot access resources on a server named Server5. All other hosts on subnet A are able to access resources on Server5.

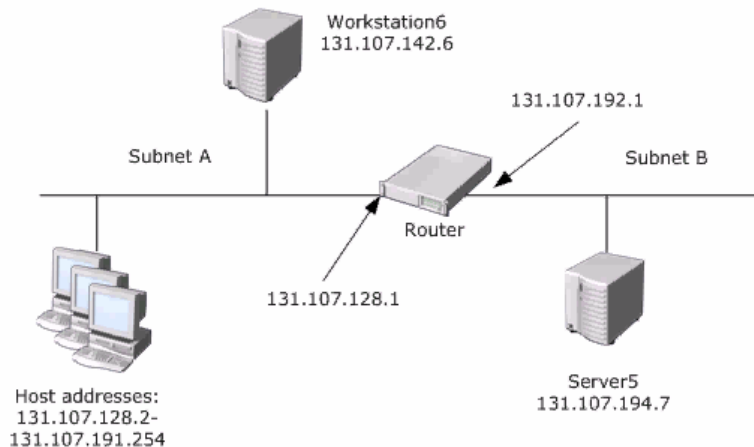
From Workstation6 you successfully ping the IP address of the router interface on the local subnet. However, you cannot ping the IP address of Server5 or the IP address of the router interface on subnet B. You run the **route print** command on Workstation6 and receive the output as shown in the following table.

Destination	Subnet mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	131.107.129.1	131.107.142.6	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
131.107.128.0	255.255.192.0	131.107.142.6	131.107.142.6	1
131.107.142.6	255.255.255.255	127.0.0.1	127.0.0.1	1
131.107.255.255	255.255.255.255	131.107.142.6	131.107.142.6	1
224.0.0.0	224.0.0.0	131.107.142.6	131.107.142.6	1
255.255.255.255	255.255.255.255	131.107.142.6	131.107.142.6	1

You need to ensure that Workstation6 can connect to Server5 and any other hosts on subnet B.

What should you do?

- A. Change the IP address on Workstation6 to 131.107.142.128.
- B. Change the subnet mask on Workstation6 to 255.255.0.0.
- C. Change the default gateway on Workstation6 to 131.107.128.1.
- D. Change the IP address of the router interface connecting to subnet A to 131.107.142.1.
- E. Change the IP address on the router interface connecting to subnet B to 131.107.194.1.



8

You are the network administrator for your company. All servers run Windows Server 2003.

You configure a server named Server2 as a Network Address Translation (NAT) server. Server2 has a single network adapter and a modem. Server2 connects to the Internet through a demand-dial connection.

Users report that when they attempt to connect to Internet Web sites, they intermittently receive the following error message: "Page not found." After waiting for several minutes, they can connect to the Web sites. These errors occur throughout the day.

You need to configure Server2 to allow users to always connect to Internet Web sites.

What should you do?

- A. Set the demand-dial connection to **Persistent**.
- B. Set the dial-out hours on the demand-dial connection to any day and any time.
- C. Set a demand-dial filter. Configure the filter for **Only allow the following traffic**. Specify a new filter for outbound port 80.
- D. Configure the demand-dial interface as the private interface.

9

You are the network administrator for your company. The network consists of a single subnet. The network contains 150 client computers and 16 servers. All computers on the network use the 10.10.0.0/16 addressing scheme.

Your manager instructs you to place the 16 servers into a separate subnet that uses the 192.168.1.0 public addressing scheme. You must plan for a maximum of 30 servers in the future.

You need to configure a new subnet mask. The subnet mask must allow a sufficient number of IP addresses for the existing servers and for future server growth. However, you want to conserve addresses as much as possible.

Which subnet mask should you use?

To answer, drag the appropriate subnet mask to the correct location in the dialog box.

The image shows a drag-and-drop interface for configuring network settings. On the left, under the heading "Subnet Masks", there is a list of five possible subnet masks: 255.255.255.224, 255.255.255.240, 255.255.255.248, 255.255.255.252, and 255.255.255.254. On the right, the "Internet Protocol (TCP/IP) Properties" dialog box is open to the "General" tab. The "Use the following IP address:" radio button is selected. The IP address is set to 192.168.1.3, the default gateway to 192.168.1.1, and the DNS servers to 10.10.6.20 and 10.10.2.89. The "Subnet mask:" field is currently empty and labeled "Subnet Mask", indicating that a mask needs to be dragged into it from the list on the left. The "Advanced..." button is visible at the bottom of the dialog box.

10

You are the network administrator for your company. The network consists of a single subnet. A Windows Server 2003 computer named Server1 functions as a DHCP server.

Server1 leases IP addresses in the 10.1.1.0/24 range to desktop client computers. There are 12 client reservations for other servers and network printers. You have configured several detailed scope and server options.

If Server1 fails, you want to have a contingency plan that will allow you to use a domain controller named DC2 as a DHCP server as quickly as possible. You install DHCP on DC2 without any configuration and stop the DHCP Server service.

You want to list the tasks that are required to back up Server1 and the tasks that are required to restore the backup to DC2. A backup age of 24 hours or less is acceptable.

If Server1 fails, which set of tasks is required to enable DC2 to replace Server1 as the DHCP server?

- A. On Server1: Schedule the Backup utility to back up the System State data to tape every 24 hours.
On DC2: Perform a non-authoritative System State restore. Using the Services console, start the DHCP Server service. Authorize DHCP. Reconcile the database.
- B. On Server1: Use the Backup utility to schedule a tape backup of the DHCP database every 24 hours.
On DC2: Restore the tape backup of the DHCP database to a folder. Using the DHCP console, restore the backup from the same folder. From the command prompt, type **net start dhcpserver**. Authorize DHCP.
- C. On Server1: Schedule the Backup utility to back up the System State data to tape every 24 hours.
On DC2: Perform an authoritative System State restore. Manually re-create the server and scope options that were on Server1. From a command prompt, type **net start dhcpserver**. Authorize DHCP.
- D. On Server1: Use the DHCP console to perform a DHCP backup every 24 hours. Copy the backup on a network share that is accessible by DC2.
On DC2: Copy the backup to a local folder. Using the DHCP console, restore the backup from the local folder. From a command line, type **net start dhcp**. Authorize DHCP. Re-create the 12 client reservations.

You are the network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. All servers are configured with static IP addresses.

All client computers run Windows XP Professional. All client computers are configured as DHCP clients. The relevant portion of the network is configured as shown in the **Network** exhibit. (Click the **Exhibit** button.)

A user named Maria reports that she cannot access network resources by using her client computer. Her client computer is named Client2. Maria reports that she received an error message about a duplicate address on the network when she started her computer this morning.

You examine the DHCP scope properties on the DHCP server. The scope properties are shown in the **DHCP** exhibit. (Click the **Exhibit** button.)

You need to ensure that Maria can access the network by using her client computer. You also need to ensure that this problem will not recur.

What should you do?

- A. Exclude the IP addresses 192.168.10.10 to 192.168.10.15 from the DHCP scope. Restart Client2.
- B. Add the additional IP addresses 192.168.10.201 to 192.168.10.250 to the DHCP scope. Restart Client2.
- C. Configure the DHCP scope to detect IP address conflicts. Restart Client2.
- D. Reconcile the DHCP scope on the DHCP server. Restart Client2.

