IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **070-293**

Title : Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

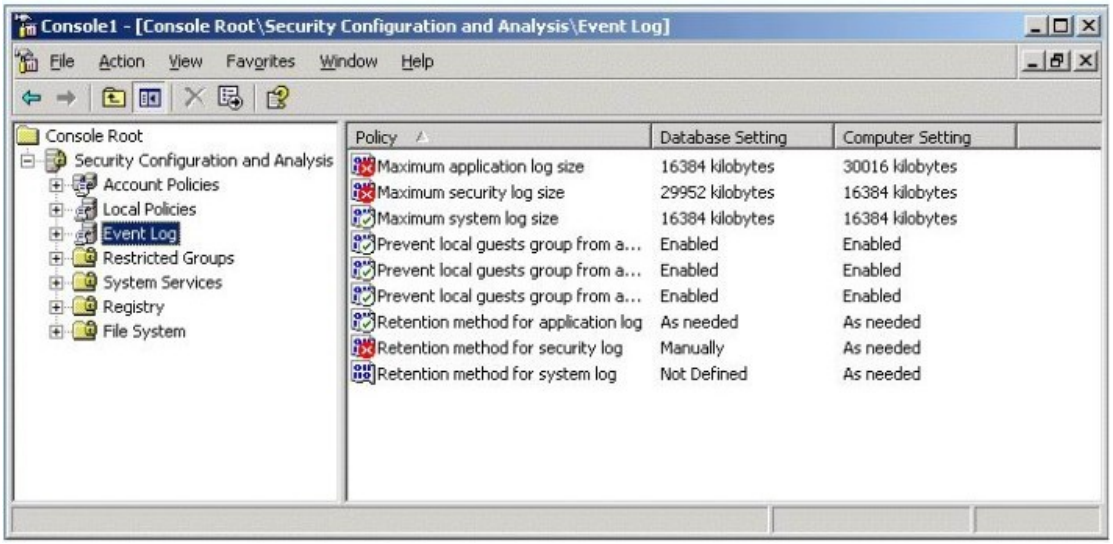
Version : Demo

1.You are the network administrator for your company. The network consists of a single Active Directory domain. The network contains two Windows Server 2003 domain controllers, two Windows 2000 Server domain controllers, and two Windows NT Server 4.0 domain controllers.
All file servers for the finance department are located in an organizational unit (OU) named Finance Servers. All file servers for the payroll department are located in an OU named Payroll Servers. The Payroll Servers OU is a child OU of the Finance Servers OU.
The company's written security policy for the finance department states that departmental servers must have security settings that are enhanced from the default settings. The written security policy for the payroll department states that departmental servers must have enhanced security settings from the default settings, and auditing must be enabled for file or folder deletion.
You need to plan the security policy settings for the finance and payroll departments.
What should you do?
A.Create a Group Policy object (GPO) to apply the Compatws.inf security template to computer objects, and link it to the Finance Servers OU.
Create a second GPO to enable the Audit object access audit policy on computer objects, and link it to the Payroll Servers OU.
B.Create a Group Policy object (GPO) to apply the Securews.inf security template to computer objects, and link it to the Finance Servers OU.
Create a second GPO to enable the Audit object access audit policy on computer objects, and link it to the Payroll Servers OU.
C.Create a Group Policy object (GPO) to apply the Compatws.inf security template to computer objects, and link it to the Finance Servers OU.
Create a second GPO to apply the Hisecws.inf security template to computer objects, and link it to the Payroll Servers OU.
D.Create a Group Policy object (GPO) to apply the Securews.inf security template to computer objects, and link it to the Finance Servers and to the Payroll Servers OUs.
Create a second GPO to enable the Audit object access audit policy on computer objects, and link it to the Payroll Servers OU.
Answer:B

2.You are the network administrator for your company. The network consists of a single Active Directory domain. The functional level of the domain is Windows Server 2003. The domain contains an organizational unit (OU) named Servers that contains all of the company's Windows Server 2003 resource servers. The domain also contains an OU named Workstations that contains all of the company's Windows XP Professional client computers. You configure a baseline security template for resource servers named Server.inf and a baseline security template for client computers named Workstation.inf. The Server.inf template contains hundreds of settings, including file and registry permission settings that have inheritance propagation enabled. The Workstation.inf template contains 20 security settings, none of which contain file or registry permissions settings. The resource servers operate at near capacity during business hours. You need to apply the baseline security templates so that the settings will be periodically enforced. You need to accomplish this task by using the minimum amount of administrative effort and while minimizing the performance impact on the resource servers. What should you do.?
A. Create a Group Policy object (GPO) and link it to the domain. Import both the Server.inf and the

Workstation.inf templates into the GPO.
B. Import both the Server.inf and the Workstation.inf templates into the Default Domain Policy Group Policy object (GPO).
C. On each resource server, create a weekly scheduled task to apply the Server.inf settings during off-peak hours by using the secedit command. Create a Group Policy object (GPO) and link it to the Workstations OU. Import the Workstation.inf template into the GPO.
D. On each resource server, create a weekly scheduled task to apply the Server.inf settings during off-peak hours by using the secedit command. Import the Workstation.inf template into the Default Domain Policy Group Policy object (GPO).
Answer: C

3. You are the network administrator for your company. The network consists of a single Active Directory domain. The company's written security policy requires that computers in a file server role must have a minimum file size for event log settings. In the past, logged events were lost because the size of the event log files was too small. You want to ensure that the event log files are large enough to hold history. You also want the security event log to be cleared manually to ensure that no security information is lost. The application log must clear events as needed. You create a security template named Fileserver.inf to meet the requirements. You need to test each file server and take the appropriate corrective action if needed. You audit a file server by using Fileserver.inf and receive the results shown in the exhibit. (Click the Exhibit button.) You want to make only the changes that are required to meet the requirements. Which two actions should you take? (Each correct answer presents part of the solution. Choose two.)



A. Correct the Maximum application log size setting on the file server.
B. Correct the Maximum security log size setting on the file server.
C. Correct the Maximum system log size setting on the file server.
D. Correct the Retention method for application log setting on the file server.
E. Correct the Retention method for security log setting on the file server.
F. Correct the Retention method for system log setting for the file server.
Answer: B E

4. You are the network administrator for your company. The network consists of a single Active Directory

domain. The network contains 10 domain controllers and 50 servers in application server roles. All servers run Windows Server 2003. The application servers are configured with custom security settings that are specific to their roles as application servers. Application servers are required to audit account logon events, object access events, and system events. Application servers are required to have passwords that meet complexity requirements, to enforce password history, and to enforce password aging. Application servers must also be protected against man-in-the-middle attacks during authentication. You need to deploy and refresh the custom security settings on a routine basis. You also need to be able to verify the custom security settings during audits. What should you do?
A. Create a custom security template and apply it by using Group Policy.
B. Create a custom IPSec policy and assign it by using Group Policy.
C. Create and apply a custom Administrative Template.
D. Create a custom application server image and deploy it by using RIS.
Answer: A

5.You are the network administrator for your company. All servers run Windows Server 2003. You configure a baseline security template named Baseline.inf. Several operations groups are responsible for creating templates containing settings that satisfy operational requirements. You receive the templates shown in the following table.

Operations group	Template name	Applies to
File and Print	File.inf	File servers
Database	Db.inf	Database servers
Security	Sec.inf	All resource servers

The operations groups agree that in the case of conflicting settings, the priority order listed in the following table establishes the resultant setting.

Template	Priority
Sec.inf	1
Baseline.inf	2
Specific server role template	3

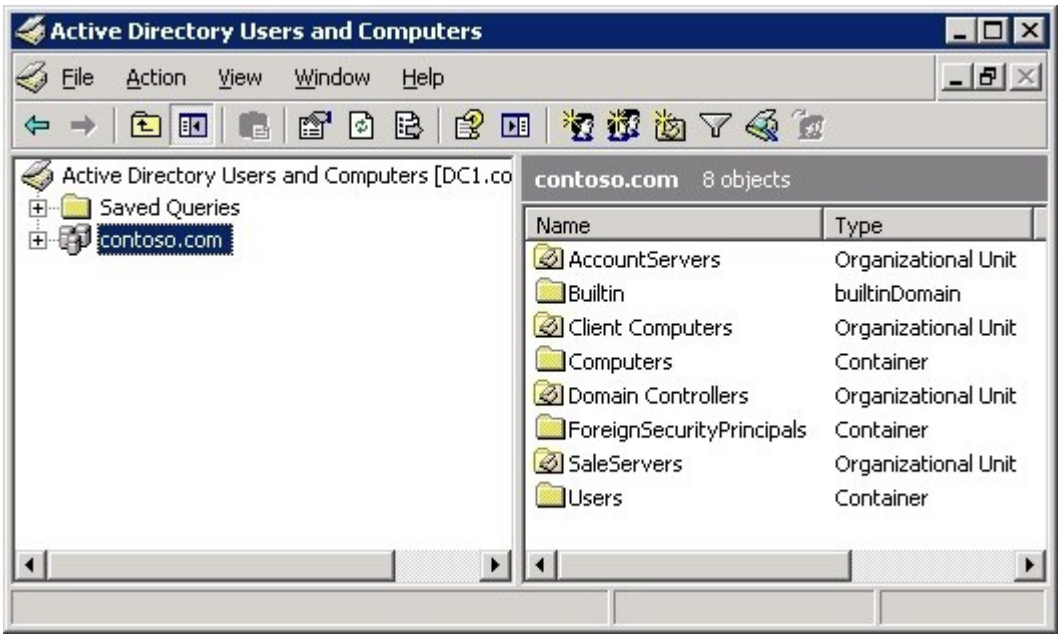
You need to create one or more Group Policy objects (GPOs) to implement the security settings. You want to minimize the amount of administrative effort required when changes are requested by the various operations groups. What should you do?
A. Create a GPO and import the following templates in the following order. Baseline.inf, Sec.inf. Create a GPO for each server role and import only the specific template for that role into each respective GPO.
B. Create a GPO and import the following templates in the following order. Sec.inf, Baseline.inf. Create a GPO for each server role and import only the specific template for that role into each respective GPO.
C. Create a GPO for each server role and import the following templates in the following order. Baseline.inf, specific server role template, Sec.inf.
D.Create a GPO and import the following templates in the following order. Sec.inf, Db.inf, File.inf, Baseline.inf.
Answer: A

6. You are the network administrator for your company. The network consists of a single Active Directory

domain. All servers run Windows Server 2003.
The network contains servers that have Terminal Server enabled. The terminal servers host legacy applications that currently require users to be members of the Power Users group.
A new requirement in the company's written security policy states that the Power Users group must be empty on all resource servers.
You need to maintain the ability to run the legacy applications on the terminal servers when the new security requirement is implemented.
What should you do?
A. Add the Domain Users global group to the Remote Desktop Users built-in group in the domain.
B. Add the Domain Users global group to the Remote Desktop Users local group on each terminal server.
C. Modify the Compatws.inf security template settings to allow members of the local Users group to run the applications. Import the security template into the Default Domain Controllers Policy Group Policy object (GPO).
D. Modify the Compatws.inf security template settings to allow members of the local Users group to run the applications. Apply the modified template to each terminal server.
Answer: D

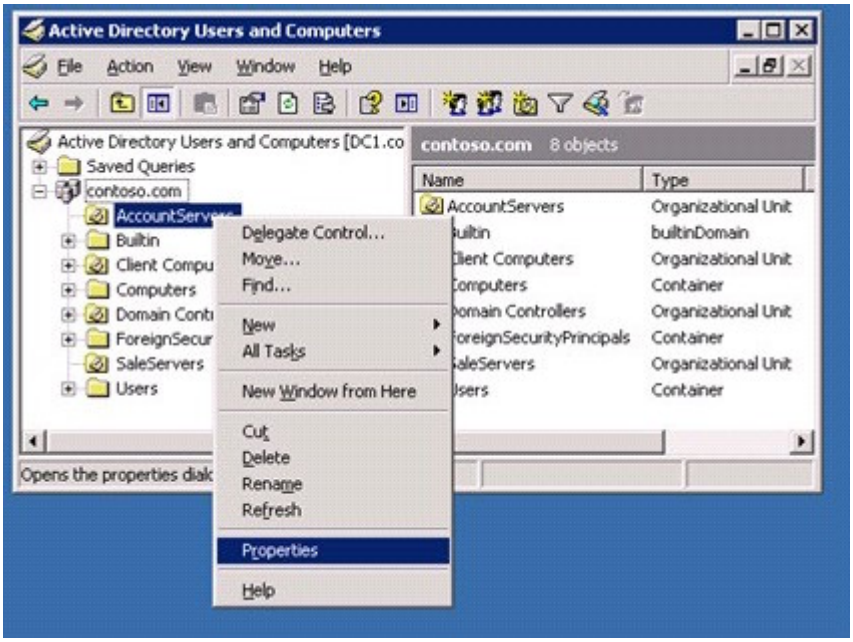
7. You are a network administrator for your company. All domain controllers run Windows Server 2003. The network contains 50 Windows 98 client computers, 300 Windows 2000 Professional computers, and 150 Windows XP Professional computers. According to the network design specification, the Kerberos version 5 authentication protocol must be used for all client computers on the internal network. You need to ensure that Kerberos version 5 authentication is used for all client computers on the internal network.
What should you do?
A. On each domain controller, disable Server Message Block (SMB) signing and encryption of the secure channel traffic.
B. Replace all Windows 98 computers with new Windows XP Professional computers.
C. Install the Active Directory Client Extensions software on the Windows 98 computers.
D. Upgrade all Windows 98 computers to Windows NT Workstation 4.0.
Answer: B

8.You are a network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003.
All file servers for the Sales department are located in an organizational unit (OU) named SaleServers. All file servers for the Accounting department are located in an OU named AccountServers.
You create a Group Policy Object (GPO) named SaleServersPolicy and link it to the SaleServers OU. You create a GPO named AccountServersPolicy and link it to the AccountServers OU.
You need to ensure that only the AccountServersPolicy settings are applied to the AccountServers OU. You must accomplish this task by using the Active Directory Users and Computers console. Your operation must not affect other settings.
Answer.CP1 AND CP2
Step #1.
Open Active Directory Users and Computers by clicking Start > Administrative Tools > Active Directory Users and Computers.



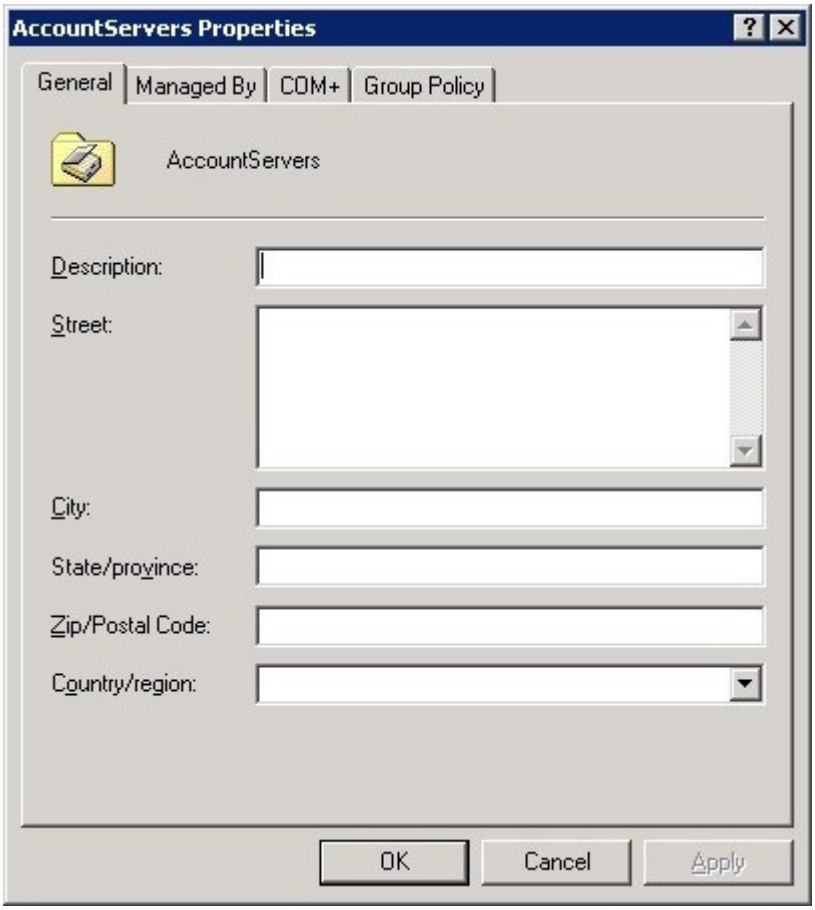
Step #2.

Expand the tree to show the Organizations Units (OUs). Right click on the AccountServers OU and select Properties.



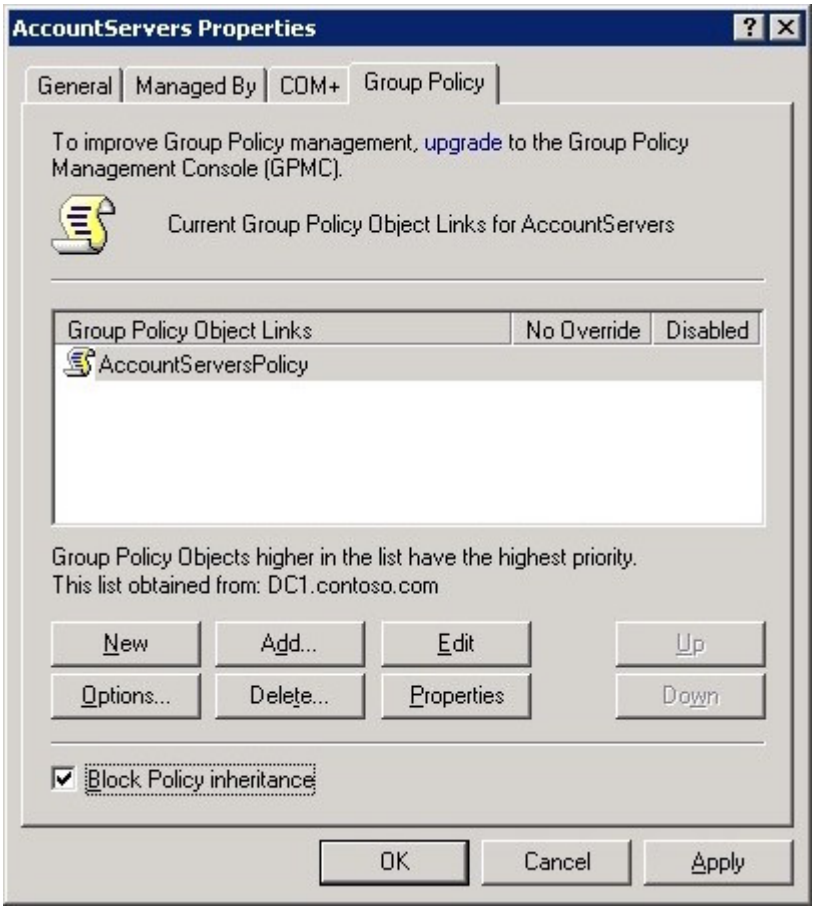
Step #3.

Go to the Group Policy tab.



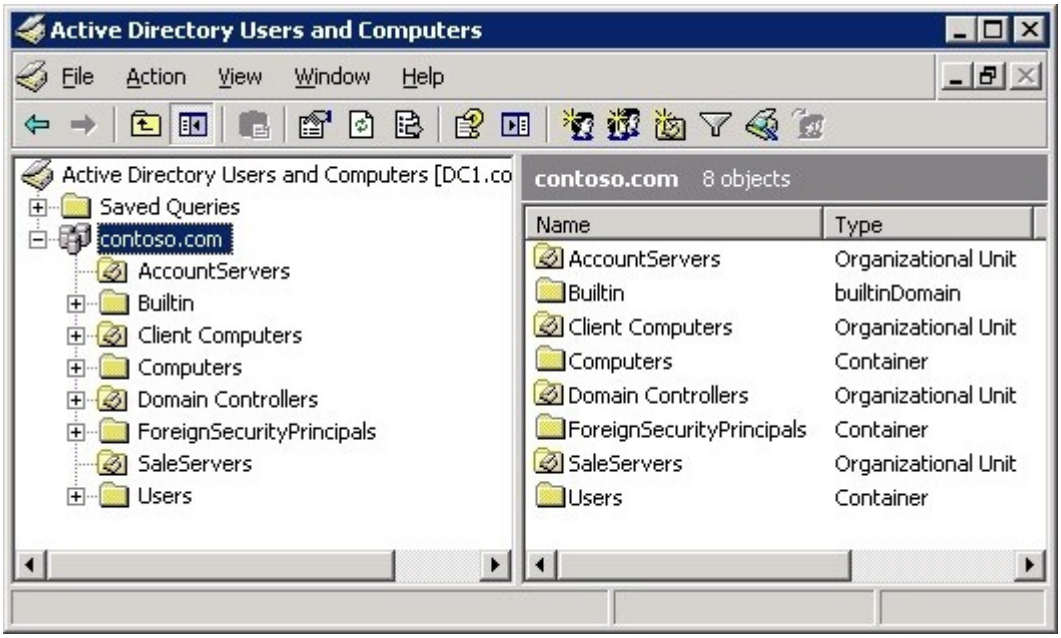
Step #4.

Tick the Block Policy Inheritance checkbox then click Apply and OK.



Step #5.

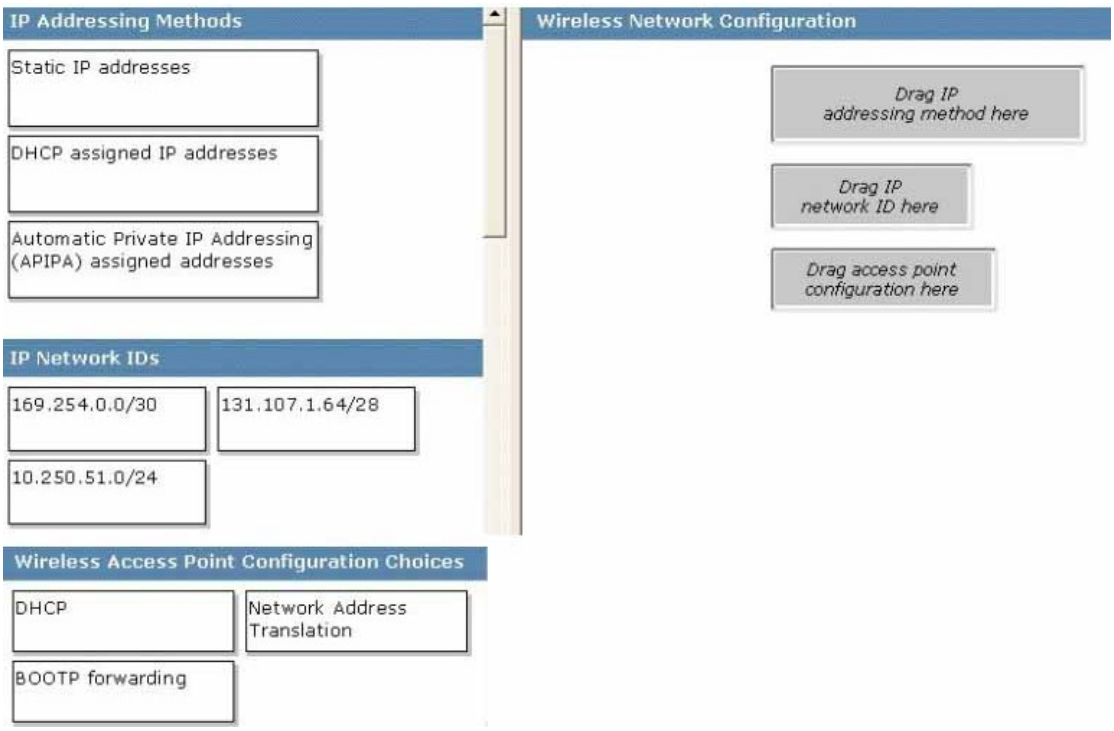
Close Active Directory Users and Computers.



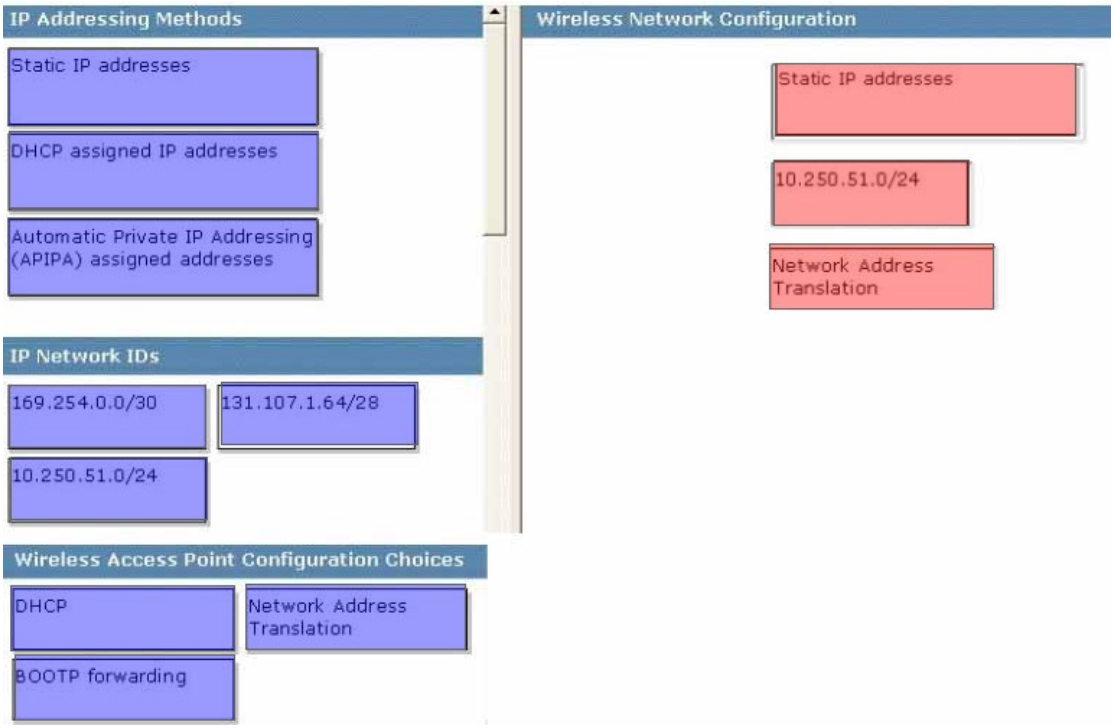
9.You are the network administrator for Tailspin Toys. The company has a main office and two branch offices. The network in the main office contains 10 servers and 100 client computers. Each branch office contains 5 servers and 50 client computers. Each branch office is connected to the main office by a direct

T1 line. The network design requires that company IP addresses must be assigned from a single classful private IP address range. The network is assigned a class C private IP address range to allocate IP addresses for servers and client computers. Tailspin Toys acquires a company named Wingtip Toys. The acquisition will increase the number of servers to 20 and the number of client computers to 200 in the main office. The acquisition is expected to increase the number of servers to 20 and the number of client computers to 200 in the branch offices. The acquisition will also add 10 more branch offices. After the acquisition, all branch offices will be the same size. Each branch office will be connected to the main office by a direct T1 line. The new company will follow the Tailspin Toys network design requirements. You need to plan the IP addressing for the new company. You need to comply with the network design requirement. What should you do?
A. Assign the main office and each branch office a new class A private IP address range.
B. Assign the main office and each branch office a new class B private IP address range.
C. Assign the main office and each branch office a subnet from a new class B private IP address range.
D.Assign the main office and each branch office a subnet from the current class C private IP address range.
Answer: C

10. You are a network administrator for a consulting company. You need to create a wireless network that will be used by consultants from your company at a customer location. The wireless network will consist of nine portable computers, three servers, and four wireless digital cameras. All computers and cameras can use either static or dynamic IP addressing. The cameras do not support data encryption. Both the portable computers and the servers must be able to initiate communication over the Internet to VPN servers in your company's main data center. Only the wireless access point is connected to the customer's corporate network.You need to plan the wireless IP network so that it minimizes the risk of unauthorized use of the wireless network and prevents unsolicited communication from the Internet to the hosts on the network.What should you do?To answer, drag the appropriate configuration settings to the Wireless Network Configuration.



Answer:

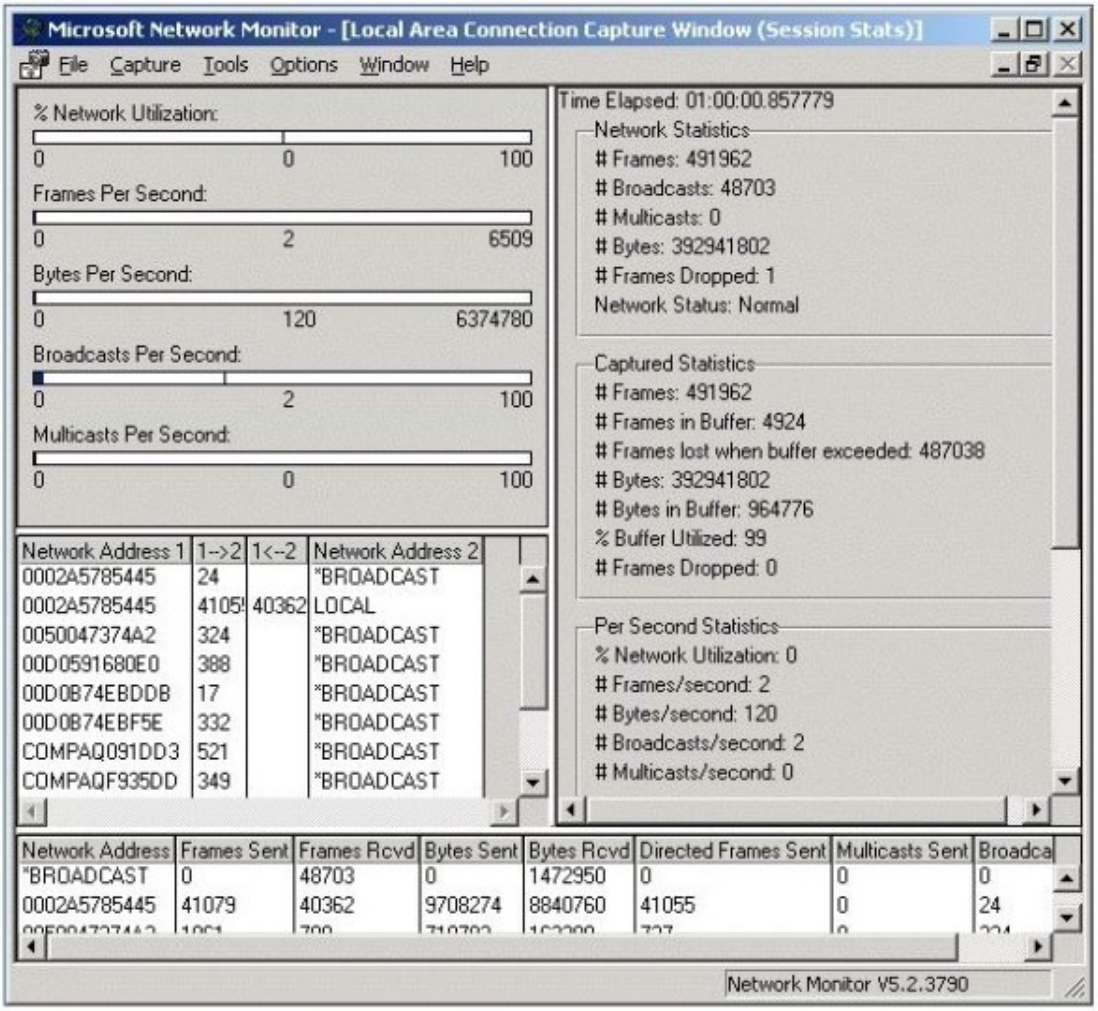


11.You are a network administrator for your company. The network consists of a single Active Directory forest that contains three domains. The functional level of the forest and of all three domains is Window Server 2003. The company has a main office and 30 branch offices. Each branch office is connected to the main office by a 56-Kbps WAN connection.
You configure the main office and each branch office as a separate Active Directory site. You deploy a Windows Server 2003 domain controller at the main office and at each branch office. Each domain controller is configured as a DNS server.
You can log on to the network from client computers in the branch offices at any time. However, users in the branch offices report that they cannot log on to the network during peak hours.
You need to allow users to log on to the network from branch office computers. You do not want to affect the performance of the branch office domain controllers. You need to minimize Active Directory replication traffic across the WAN connections.
What should you do?
A.Use Active Directory Sites and Services to enable universal group membership caching for each branch office site.
B.Use the DNS console to configure the branch office DNS servers to forward requests to a DNS server in the main office.
C.Use Active Directory Sites and Services to configure each branch office domain controller as a global catalog server.
D.Use the DNS console to configure the branch office DNS servers to use an Active Directory-integrated zone.
Answer:A

12.You are the network administrator for your company. The network contains an application server

running Windows Server 2003.
Users report that the application server intermittently responds slowly. When the application server is responding slowly, requests that normally take 1 second to complete take more than 30 seconds to complete. You suspect that the slow server response is because of high broadcast traffic on the network. You need to plan how to monitor the application server and to have a message generated when broadcast traffic is high. You also want to minimize the creation of false alarms when nonbroadcast traffic is high.
What should you do?
A.Use the Alerts option in the Performance Logs and Alerts snap-in to configure an alert to trigger when the Datagrams/sec counter in the UDPv4 object is high.
B.Use System Monitor and configure it to monitor the Segments/sec counter in the TCPv4 object.
C.Use System Monitor and configure it to monitor the Datagrams/sec counter in the UDPv4 object.
D.Use the Alerts option in the Performance Logs and Alerts snap-in to configure an alert to trigger when the Datagrams/sec counter in the TCPv4 object is high.
Answer:A

13.You are the network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003.
When the network was designed, the design team set design specifications. After the network was implemented, the deployment team set baseline specifications. The specifications for broadcast traffic are:
The design specification requires that broadcast traffic must be 5 percent or less of total network traffic.
The baseline specification showed that the broadcast traffic is always 1 percent or less of total network traffic during normal operation.
You need to monitor the network traffic and find out if the level of broadcast traffic is within design and baseline specifications. You decide to use Network Monitor. After monitoring for 1 hour, you observe the results shown in the exhibit. (Click the Exhibit button.)



You need to report the results of your observations to management.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two.)
A.Report that broadcast traffic is outside of the baseline specification.
B.Report that broadcast traffic is outside of the design specification.
C.Report that broadcast traffic is within the design specification.
D.Report that broadcast traffic is within the baseline specification.
Answer:A,B

14.You are the systems engineer for Contoso, Ltd. The internal network consists of a Windows NT 4.0 domain. The company maintains a separate network that contains publicly accessible Web and mail servers. These Web and mail servers are members of a DNS domain named contoso.com. The contoso.com zone is hosted by a UNIX-based DNS server running BIND 4.8.1.
Contoso, Ltd., is planning to migrate to a Windows Server 2003 Active Directory domain-based network. The migration plan states that all client computers will be upgraded to Windows XP Professional and that all servers will be replaced with new computers running Windows Server 2003.
The migration plan specifies the following requirements for DNS in the new environment:
Active Directory data must not be accessible from the Internet.
The DNS namespace must be contiguous to minimize confusion for users and administrators.
Users must be able to connect to resources in the contoso.com domain.

Users must be able to connect to resources located on the Internet.
The existing UNIX-based DNS server will continue to host the contoso.com domain.
The existing UNIX-based DNS server cannot be upgraded or replaced.
You plan to install a Windows Server 2003 DNS server on the internal network.
You need to configure this Windows-based DNS server to meet the requirements specified in the migration plan.
What should you do?
A.Create a primary zone named ad.contoso.com on your Windows-based DNS server. Create a delegation record for the new zone on the UNIX-based DNS server. Configure forwarders on your Windows-based DNS server.
B.Create a primary zone named ad.contoso.com on the UNIX-based DNS server. Create a secondary zone on your Windows-based DNS server for the ad.contoso.com domain.
C.Create a primary zone named contoso-ad.com on your Windows-based DNS server. Create a secondary zone on the UNIX-based DNS server for the contoso-ad.com domain.
D.Create a primary zone named contoso-ad.com on the UNIX-based DNS server. Create a stub zone on the Windows-based DNS server for the contoso-ad.com domain. Configure conditional forwarders on your Windows-based DNS server for the contoso-ad.com and contoso.com domains.
Answer:A

15.You are the network administrator for your company. The network contains Windows Server 2003 computers and Windows XP Professional computers.
The company deploys two DNS servers. Both DNS servers run Windows Server 2003. One DNS server is inside of the corporate firewall, and the other DNS server is outside of the firewall. The external DNS server provides name resolution for the external Internet name of the company on the Internet, and it is configured with root hints. The internal DNS server hosts the DNS zones related to the internal network configuration, and it is not configured with root hints.
You want to limit the exposure of the client computers to DNS-related attacks from the Internet, without limiting their access to Internet-based sites.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two.)
A.Configure the client computers to use only the internal DNS server.
B.Configure the client computers to use both DNS servers. List the internal DNS server first.
C.Configure the firewall to allow only network traffic on the DNS ports.
D.On the internal DNS server, disable recursion.
E.On the internal DNS server, configure the external DNS server as forwarder.
F.On the internal DNS server, add the external DNS server as the only root hint.
Answer:A , E

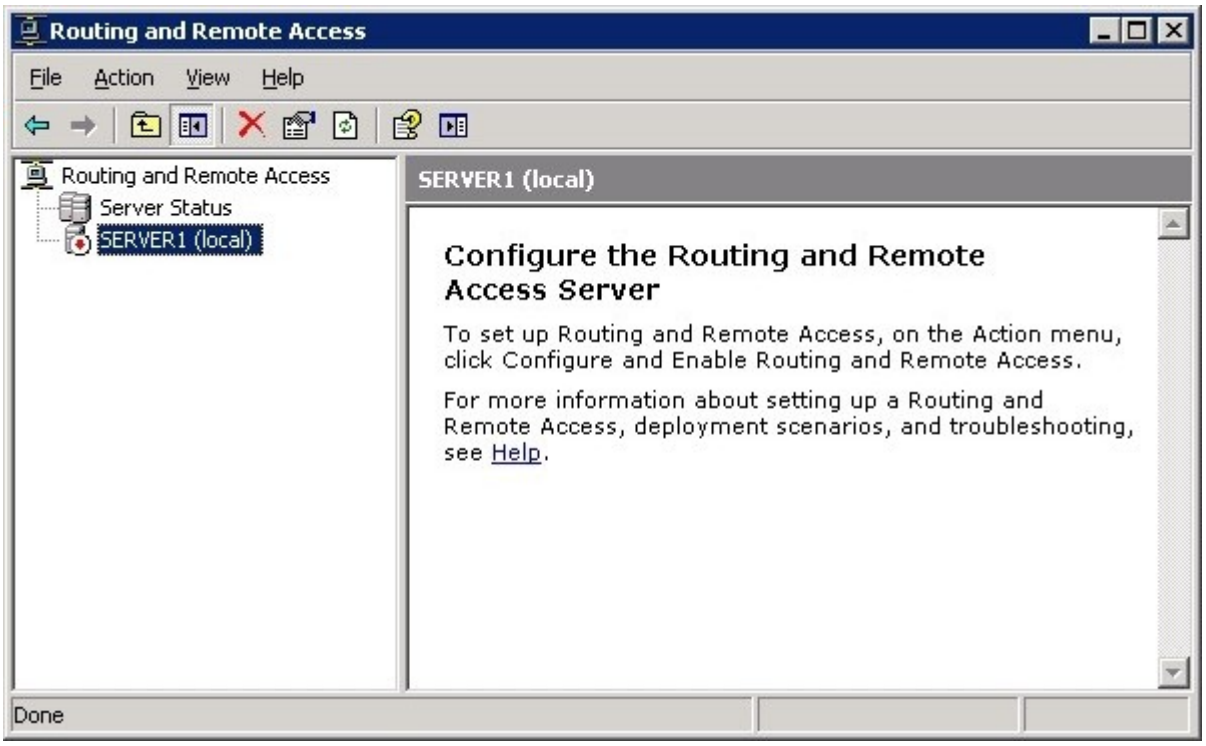
16.You are the administrator for your company. The company has a new server which runs Windows Server 2003 named Server1.
Server1 has two network connections. Internet connection is used to connect to the Internet and Local Area Network connection is used to connect to the company network.
You need to ensure that company users can access the Internet through Server1. You also need to prevent external, unauthorized users from accessing Server1 through the Internet. You must accomplish this task by using the Routing and Remote Access Server Setup Wizard dialog box. Your operation must

not affect other settings on Server1.

Answer.CP1 AND CP2 AND CP3 AND CP4

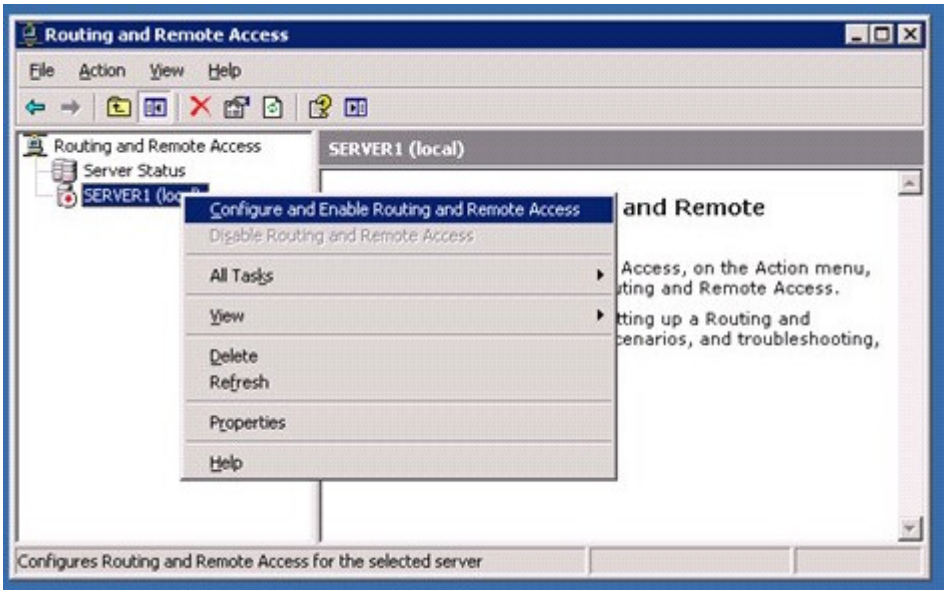
Step #1.

Open the Routing and Remote Access console by clicking Start > Administrative Tools > Routing and Remote Access.



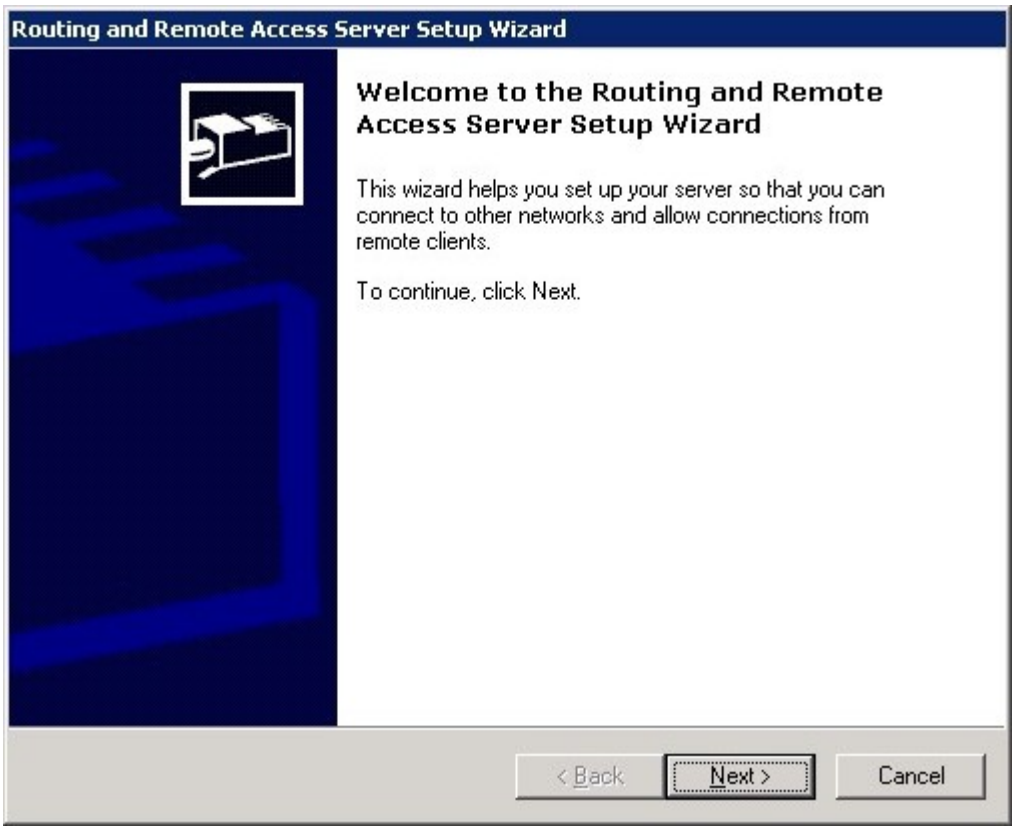
Step #2.

Right click on Server1 and select Configure and Enable Routing and Remote Access.



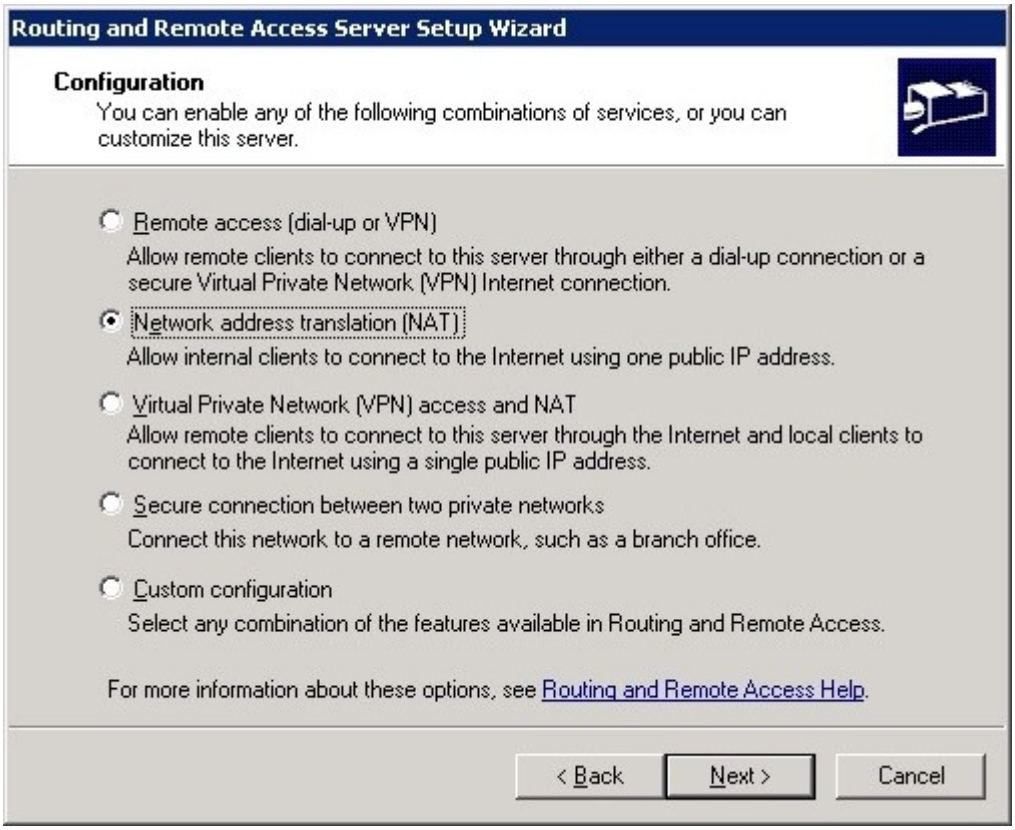
Step #3.

The Routing and Remote Access Setup Wizard will open. Click Next.



Step #4.

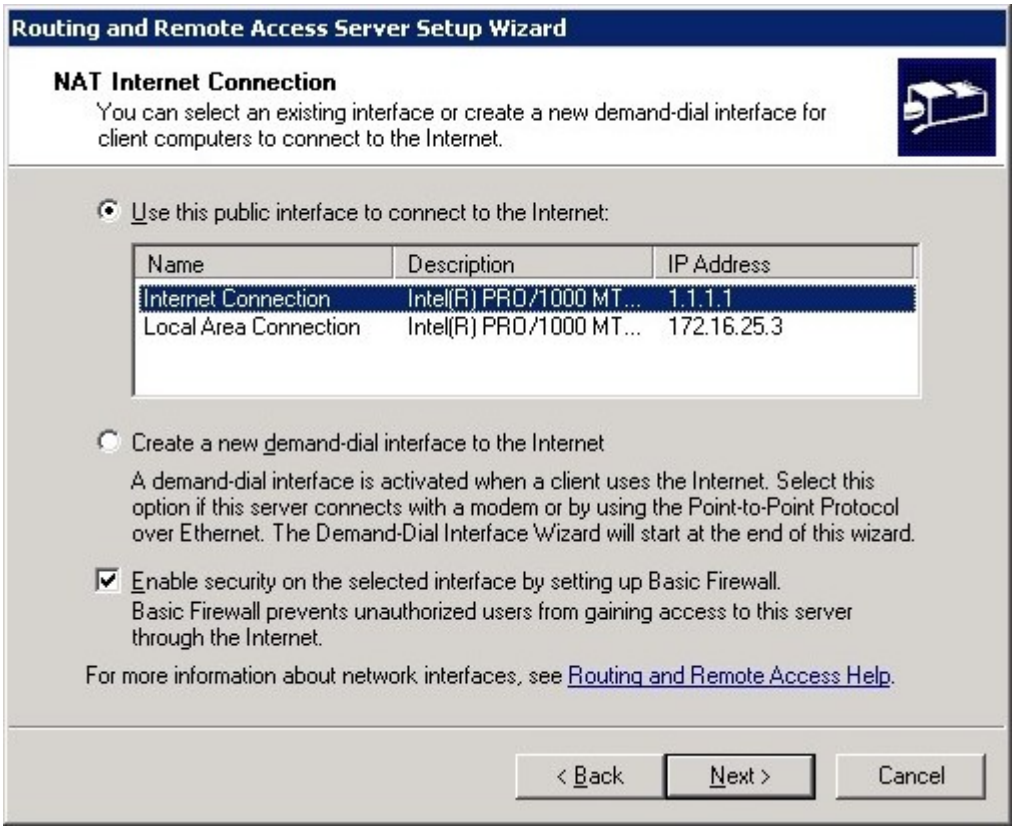
Select Network address translation (NAT) and click Next.



Step #5.

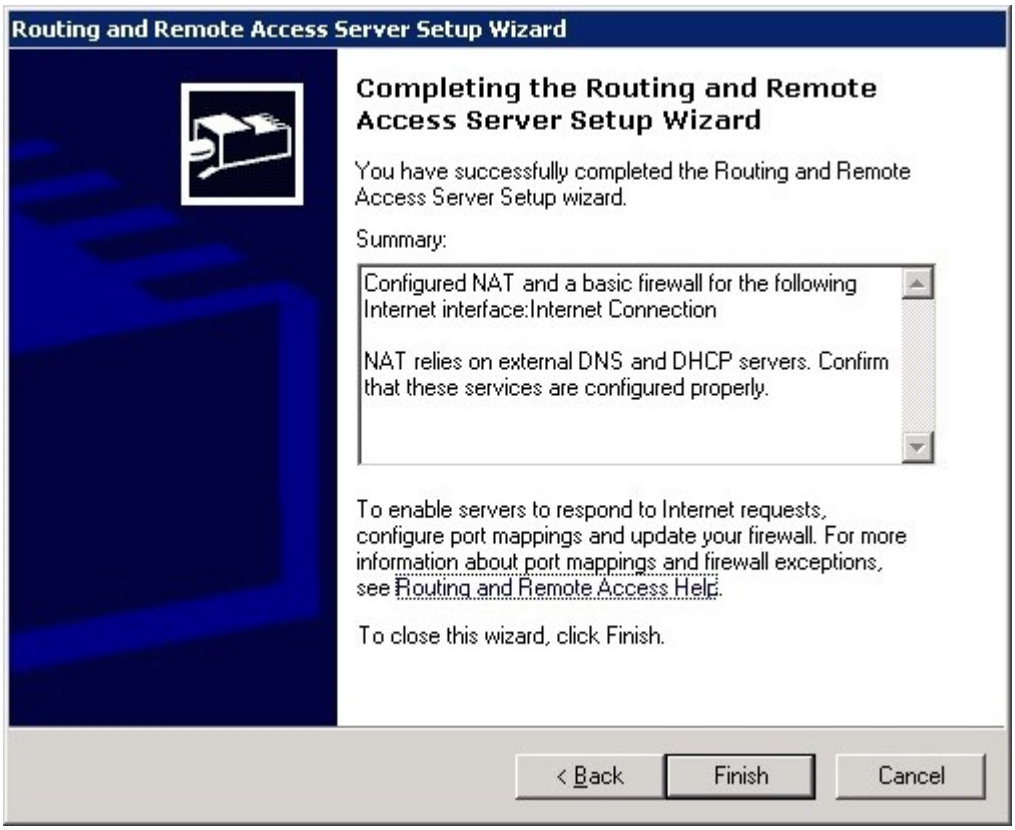
Select "Internet Connection" as the public interface. Ensure that the "Enable security on the selected

interface...." checkbox is ticked. Then click Next.



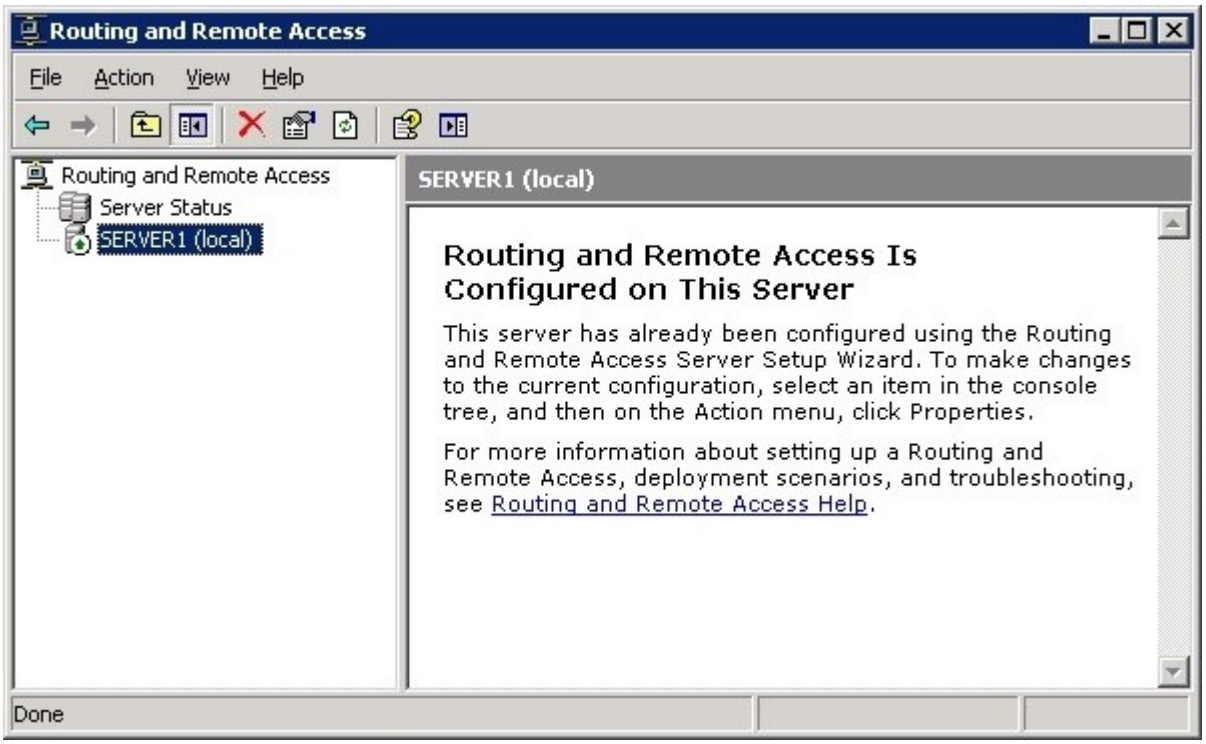
Step #6.

Click Finish to close the wizard.

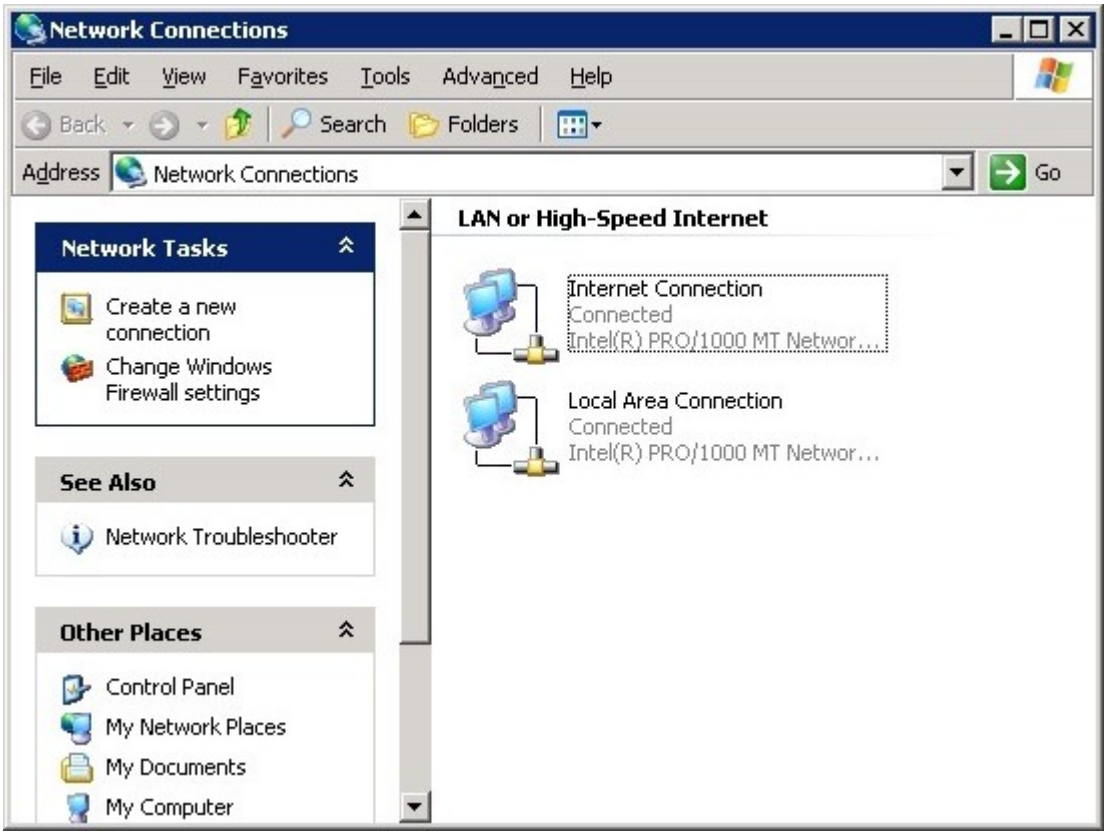


Step #7.

Close the Routing and Remote Access console.

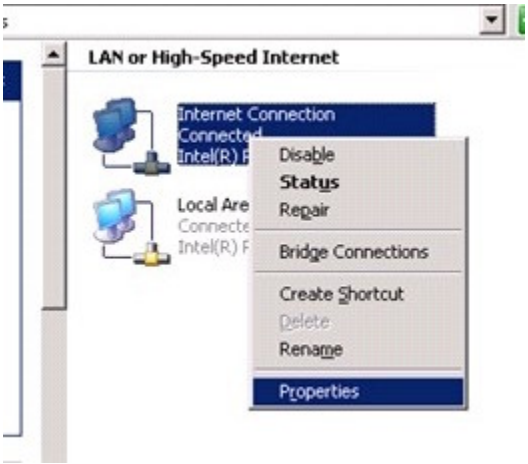


17.You are a network administrator for your company. The network contains a Windows Server 2003 computer named Server1 and ten Windows XP Professional client computers.
You configure Server1 with a LAN connection named Local Area Connection and an Internet connection named Internet Connection. All of the client computers are connected to the LAN.
The users report that they cannot connect to the Internet. You discover that the IP configuration on the client computers is correct.
You need to provide the ten client computers with Internet access. You must accomplish these tasks by using the Server1's Network Connections console with the least amount of administrative effort. Your operations must not affect other settings on Server1.
Answer.CP1 AND CP2
We need to enable Internet Connection Sharing (ICS) on the adapter named Internet Connection.
Step #1.
Open the Network Connections console by clicking Start > Control Panel > Network Connections.



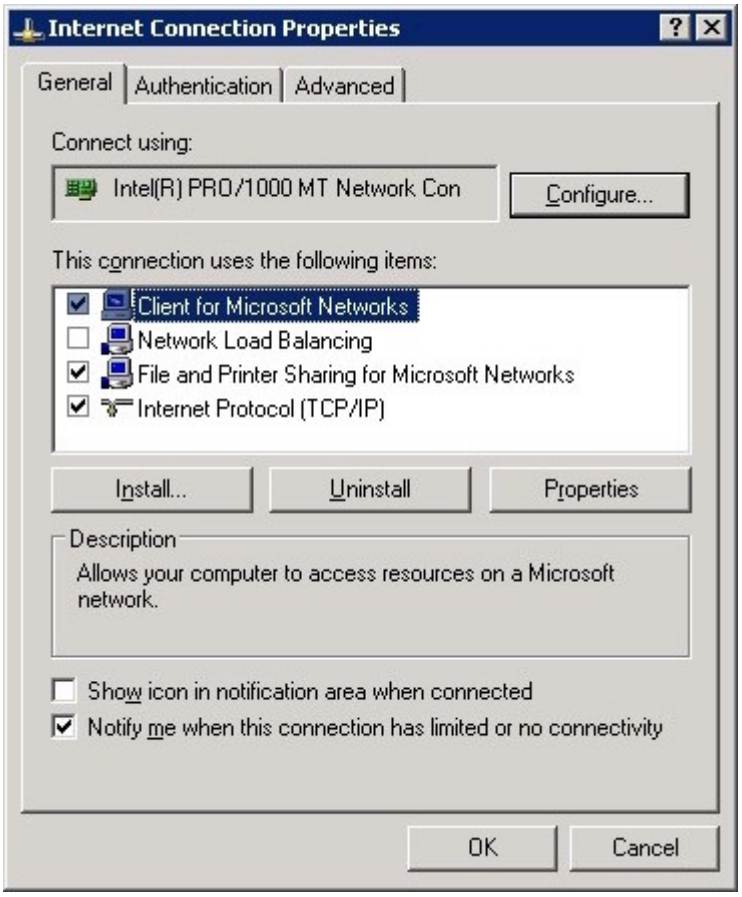
Step #2.

Right click on Internet Connection and select Properties.



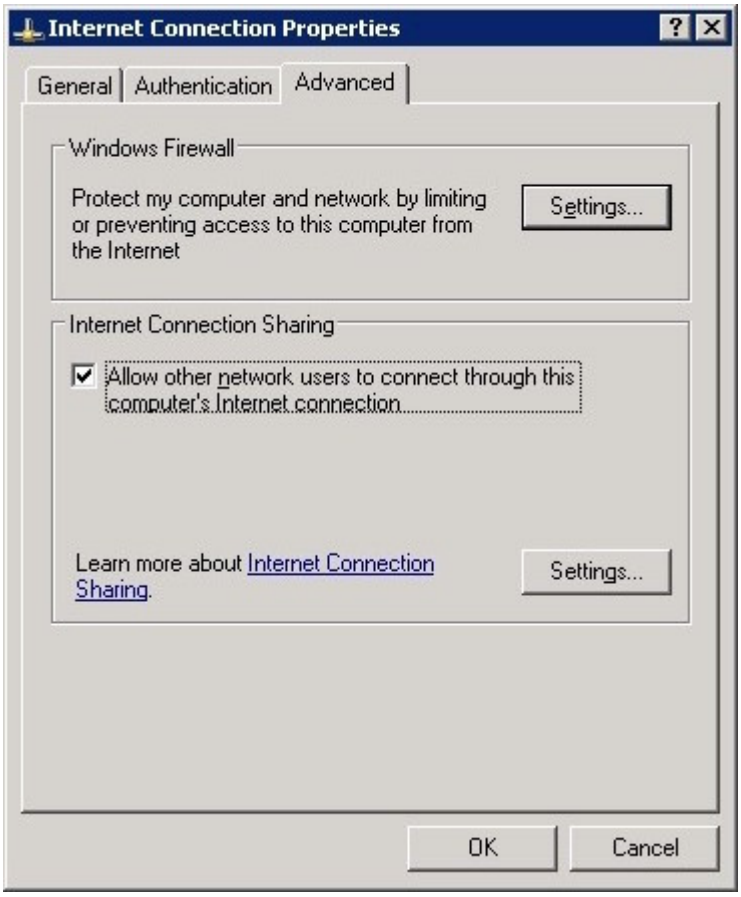
Step #3.

Click the Advanced tab.

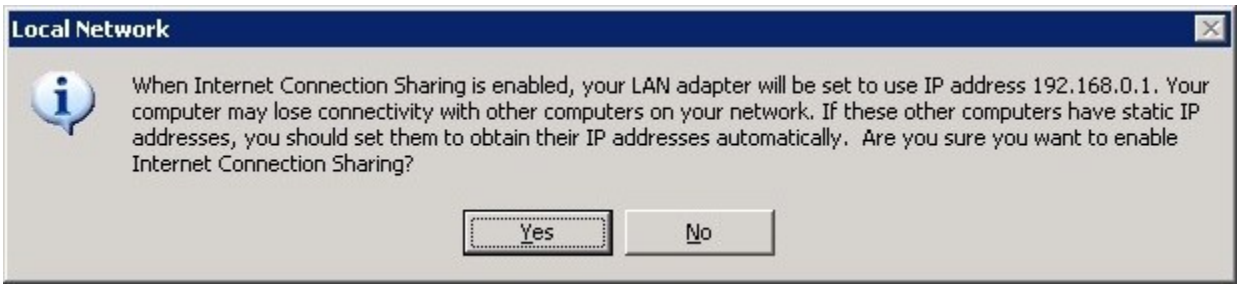


Step #4.

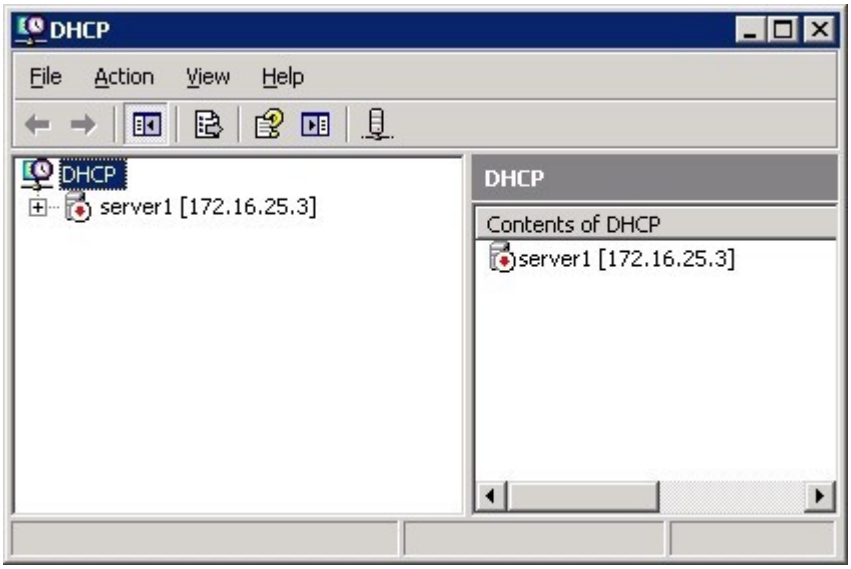
Tick the checkbox to enable Internet Connection Sharing then click OK.



Step #5.
Click Yes.

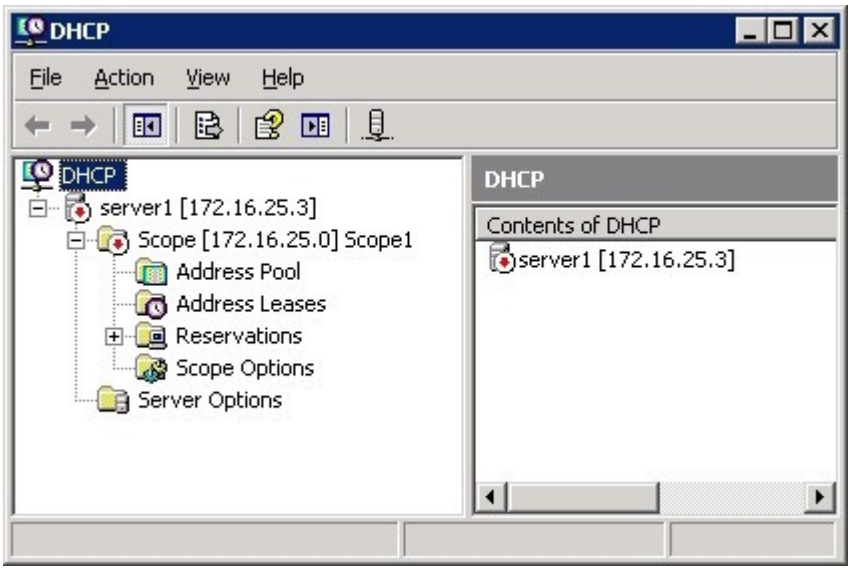


18.You are a network administrator for your company. All servers run Windows Server 2003. All client computers run Windows XP Professional.
All client computers receive their TCP/IP configuration information from the DHCP server named Server1.
You discover that client computers get a new IP address every time they are restarted.
You need to ensure that client computers receive the same IP address as often as possible regardless of a system restart. You must accomplish this task by using the DHCP console. Your operation must not affect other settings.
Answer.(CP1 OR CP2) AND CP3
We need to change the lease time to "Unlimited".
Step #1.
Open the DHCP console by clicking Start > Administrative Tools > DHCP.



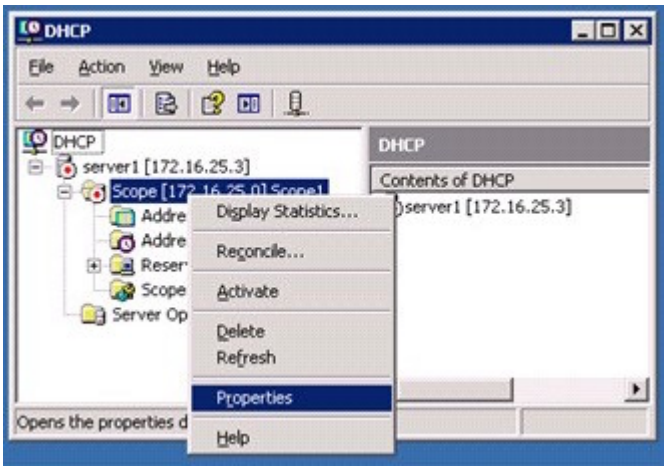
Step #2.

Expand the tree.

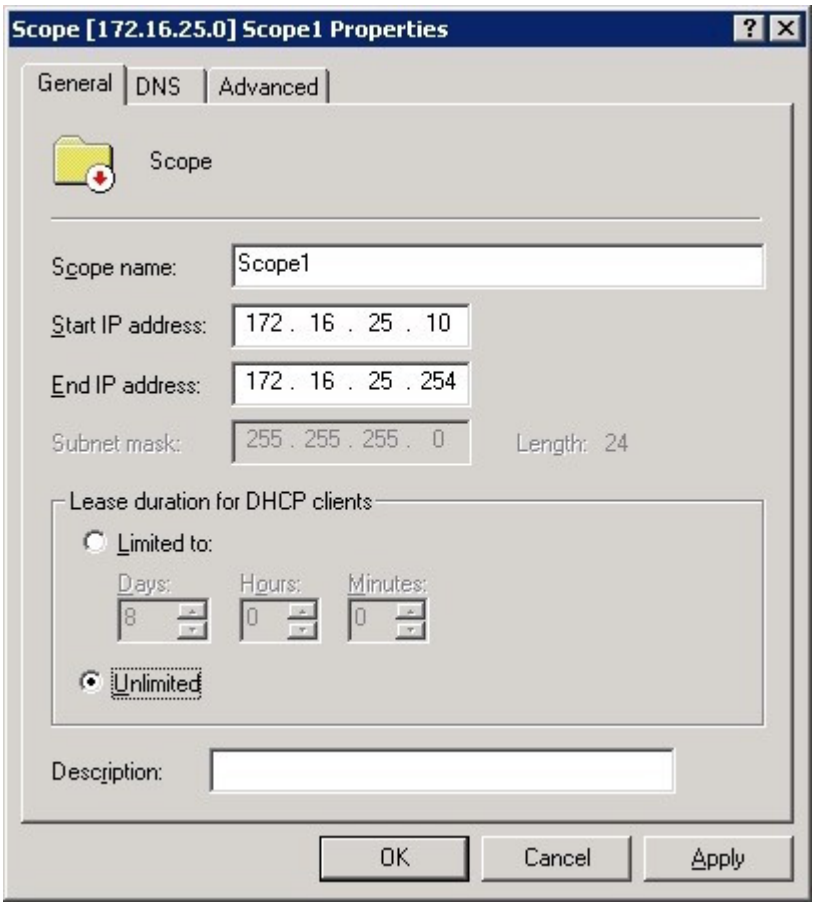


Step #3.

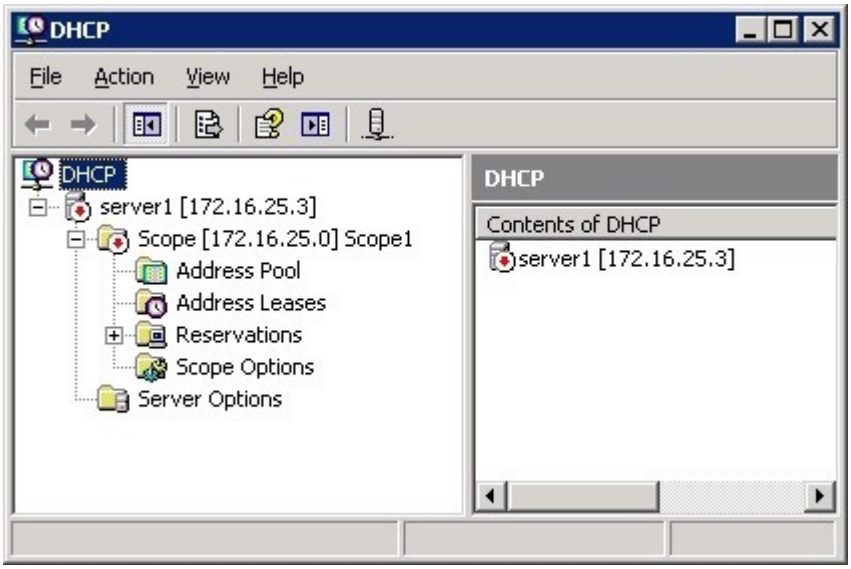
Right click on Scope1 and select Properties.



Step #4.
Select Unlimited then click Apply and OK.

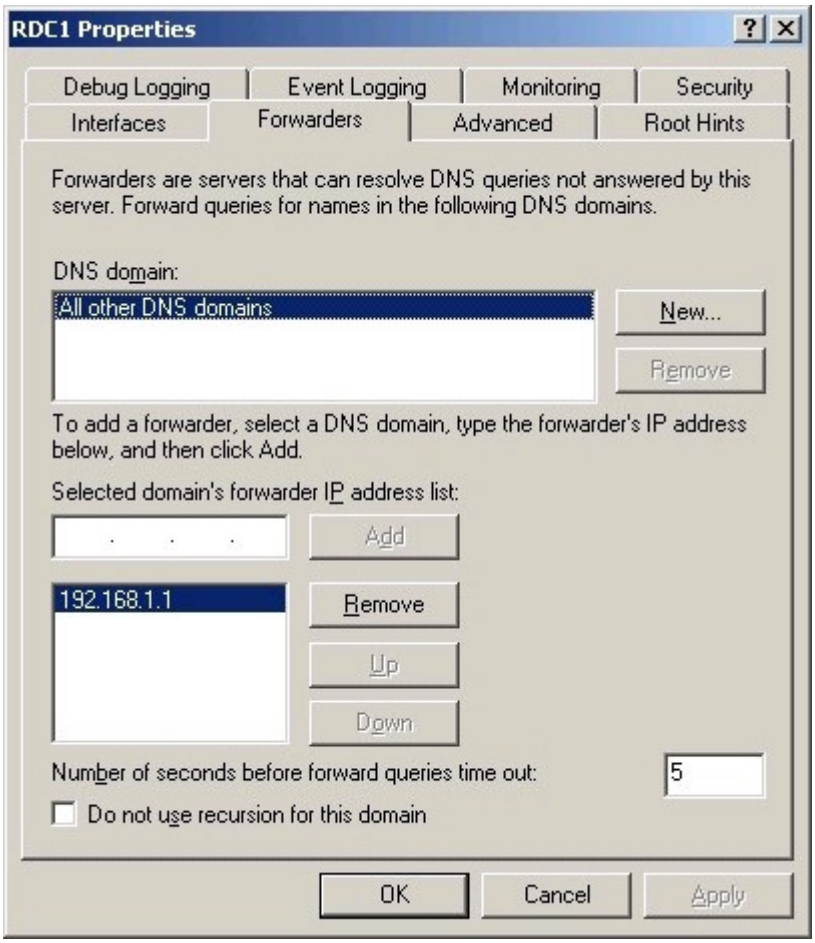


Step #5.
Close the DHCP console.



19.You are a network administrator for your company. The network consists of a single Active Directory domain named treyresearch.com. All servers run Windows Server 2003. All client computers run Windows XP Professional.

The company has two DNS servers named Server1 and Server2. Server1 hosts the primary DNS zone for treyresearch.com. Server2 provides name resolution for the external Internet name of the company on the Internet and is configured with root hints.
Client computers are configured to use Server1 as their only DNS server.
Users report that they cannot access Web sites on the Internet.
You need to ensure that the client computers can access Internet-based sites. You must accomplish this task by using Server1's DNS console with the least amount of administrative effort. Your operation must not affect other settings on Server1.
Answer.CP1 AND CP2
DNS console -> Server -> Properties -> Forwarders, 'All other DNS domains' to IP address for Server2.



20.You are a network administrator for your company. The company has a main office and one branch office. The network consists of a single Active Directory domain. All servers run Windows Server 2003.
The company needs to connect the main office network and the branch office network by using Routing and Remote Access servers at each office. The networks will be connected by a VPN connection over the Internet.
The company's written security policy includes the following requirements for VPN connections over the Internet:
All data must be encrypted with end-to-end encryption.
VPN connection authentication must be at the computer level.
Credential information must not be transmitted over the Internet as part of the authentication process.

You need to configure security for VPN connection between the main office and the branch office. You need to comply with the written security policy.
What should you do?
A.Use a PPTP connection with EAP-TLS authentication.
B.Use a PPTP connection with MS-CHAP v2 authentication.
C.Use an L2TP connection with EAP-TLS authentication.
D.Use an L2TP connection with MS-CHAP v2 authentication.
Answer:C