070-216

Implementing and Administering a Microsoft
Windows 2000 Network Infrastructure

Version 11.0

Important Note
Please Read Carefully

Study Tips
This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Further Material
For this test TestKing also provides:
* Study Guide. Concepts and labs.
* Interactive Test Engine Examinator. Check out an Examinator Demo at
http://www.testking.com/index.cfm?pageid=724

Latest Version
We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at TestKing an update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to www.testking.com
2. Click on **Member zone/Log in**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

For most updates, it is enough just to print the new questions at the end of the new version, not the whole document.

Feedback
Feedback on specific questions should be send to feedback@testking.com. You should state: Exam number and version, question number, and login ID.

Our experts will answer your mail promptly.

Copyright
Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that a particular pdf file is being distributed by you, TestKing reserves the right to take legal action against you according to the International Copyright Laws.

Leading the way in IT testing and certification tools, www.testking.com

Note 1: First customer, if any, to beat TestKing in providing answers to the unanswered questions will receive a credit equal to cost of this product. Send answers to feedback@testking.com.

Note 2: Please do not mail us to point out that there are questions without answers. We already know that. Answers will be provided in Version 11.0.

QUESTION NO: 1
You are the administrator of Windows 2000 network. The network consists of 30 Windows 2000 Professional computers, and two Windows 2000 Server computers named Athens and Boston. Athens has a permanent cable modem connection to the Internet. All Windows 2000 Professional computers on the network are configured to use Automatic Private IP addressing (APIPA). The network does not contain a DHCP server.

To allow all Windows 2000 Professional computers on the network to access the Internet through the cable modem connection of Athens, you install and configure the Network Address Translation (NAT) routing protocol on Athens.

You decide to use IP addresses in the range of 192.168.40.1 through 192.168.40.50 for the network. Athens is configured to use an IP address of 192.168.40.1.

Boston is a web server configured with an IP address of 192.168.40.2 and a default gateway of 192.168.40.1. Your Internet service provider (ISP) has allocated two IP addresses, 207.46.179.16 and 207.46.179.17 to your network. The network is shown in the exhibit.
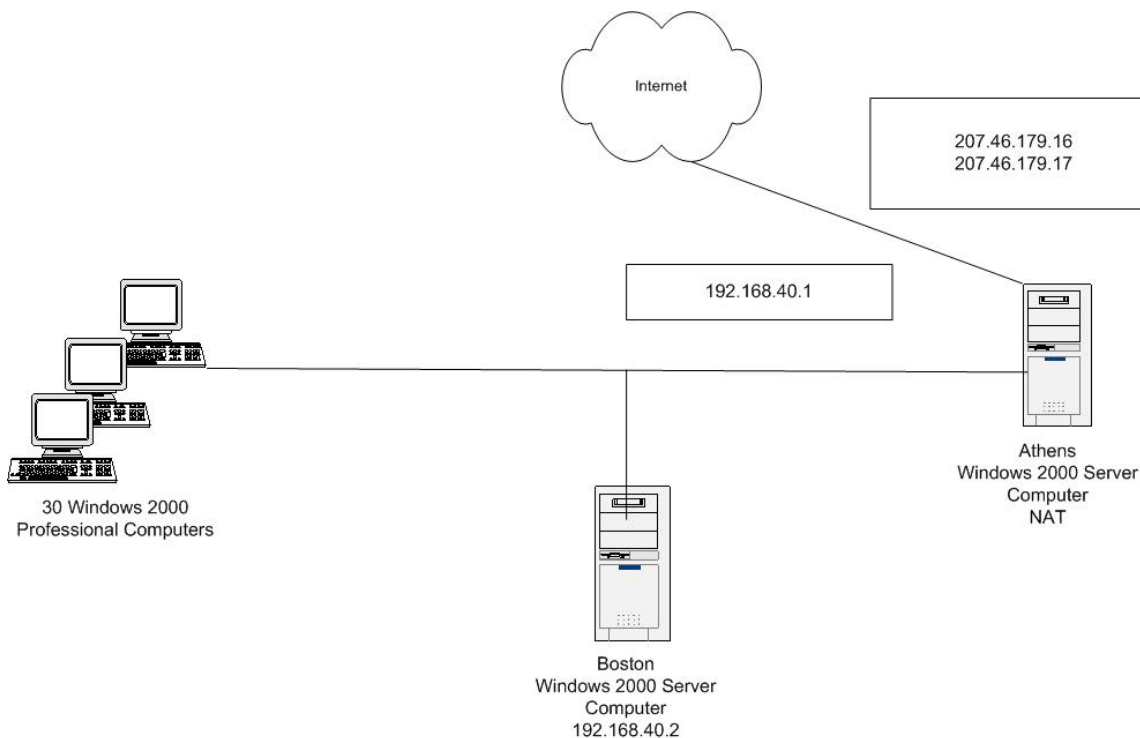
You want to allow Internet users from outside your internal network to use an IP address of
207.46.179.17 to access the resources on Boston through the NAT service on Athens.

How should you configure the network to accomplish this goal?

A. Configure Athens with a static route on the private interface of the NAT routing protocol.
    Use a destination address of 207.46.179.17, a network mask of 255.255.255.255, and a gateway of
    192.168.40.2.
B. Configure Boston with a static route on the LAN interface.
    Use a destination address of 192.168.40.1, a network mask of 255.255.255.255, and a gateway of
    207.46.179.17.
C. Configure the LAN interface of Boston to use multiple IP addresses.
    Assign the additional IP address of 207.46.179.17 to the interface.
D. Configure the public interface of the NAT routing protocol to use an address pool with a starting
    address of 207.46.179.16 and a mask of 255.255.255. 254.
    Reserve a public IP address of 207.46.179.17 for the private IP address of 192.168.40.2.

Answer: D.
Explanation: Normal network address translation (NAT) allows outbound connections from a private network
to the public network. Web browsers that run from a private network create connections to Internet resources.
The return traffic from the Internet can cross the NAT because the connection was initiated from the private
network. To allow Internet users to access resources on our private network, we must configure a static IP
address configuration on the resource server including IP address from the range of IP addresses allocated by
the NAT computer, a subnet mask also from the range of IP addresses allocated by the NAT computer, a default
gateway, which is the private IP address of the NAT computer, and a DNS server. We must exclude the IP
address being used by the resource computer from the range of IP addresses being allocated by the NAT
computer. We must also configure a special port, which is a static mapping of a public address and port number
to a private address and port number. A special port maps an inbound connection from an Internet user to a
specific address on your private network. By using a special port, we can create a Web server on our private
network that is accessible from the Internet.

Incorrect Answers:
A: NAT does not use a static route to allow inbound connects; instead a special port is used to create a
       static mapping between a public address and the private address.
B: A special port, not a static router, is used to create a static mapping. The mapping must be made on the
       NAT computer, not on the computer with the local web server (not on Boston)
C: The local web Server only requires one IP address, not two. An additional public IP address is needed to
       create the static port.

QUESTION NO: 2

You are the administrator of a Windows 2000 network. The network consists of a Windows 2000 Server computer named SrvA and 30 Windows 2000 Professional computers. SrvA has a dial-up connection that connects to the Internet.

All Windows 2000 Professional computers on the network are configured to use Automatic Private IP Addressing (APIPA). There is no DHCP server on the network.

SrvA is configured to use an IP address of 192.16.80.1. Routing and Remote Access and all the ports on SrvA are enabled for demand-dial routing. The Network Address Translation (NAT) routing protocol is added.

You want to allow all Windows 2000 Professional computers on the network to access the Internet through a translated demand-dial connection on SrvA. How should you configure the network? (Choose four)

A.	Create a new demand-dial interface for the local area connection.
B.	Create a new demand-dial interface for the dial-up connection
C.	Add a public and a private interface to the NAT routing protocol
D.	Configure the IP address of the Internet service provider (ISP) as the default gateway on the private interface.
E.	Add a default static route that uses the public interface
F.	Configure the NAT routing protocol to enable network address translation assignment and name resolution.
G.	Configure the public NAT interface with an address pool of 192. 16. 80. 1

Answer: B, C, E, F.
Explanation: To configure the NAT server we must
   1. Install and enable Routing and Remote Access service
   2. Configure the IP address of the home network interface.
       (the IP address of the LAN adapter that connects to the home network should be configured with an IP address of 192.168.0.1; a subnet mask of 255.255.255.0; and with no default gateway).
   3. Enable routing on our dial-up port.
   4. Create a demand-dial interface to connect to our ISP (B).
   5. Create a default static route that uses the public Internet interface (E).
   6. Add the NAT routing protocol.
   7. Add the public Internet and the private home interface to NAT routing protocol (C).
   8. Enable network address translation addressing and name resolution (F).

Reference: Windows 2000 Server Documentation, Deploying network address translation

Incorrect Answers:
A: The demand-dial interface must be put on the dial-up connection not the local area connection.
**D:** On the private interface the default gateway (from the clients point of view) is the NAT computer.

G: The address pool consists of public addresses. The ISP provides 1 or more public IP addresses. These addresses are added to the address pool. 192.16.80.1 is a private IP address not a public.

QUESTION NO: 3
You are the administrator of TestKing's network. To allow fault tolerance for your external DNS Server, your Internet Service Provider (ISP) hosts a DNS Server on its UNIX Server. The UNIX Server is used as the secondary DNS server for your primary external DNS Server.

Users inform you that they are not able to connect to the URL of the company's Web Server. You investigate and discover that this inability to connect occurs during times when your primary external DNS Server is unavailable.
What should you do to resolve this problem?
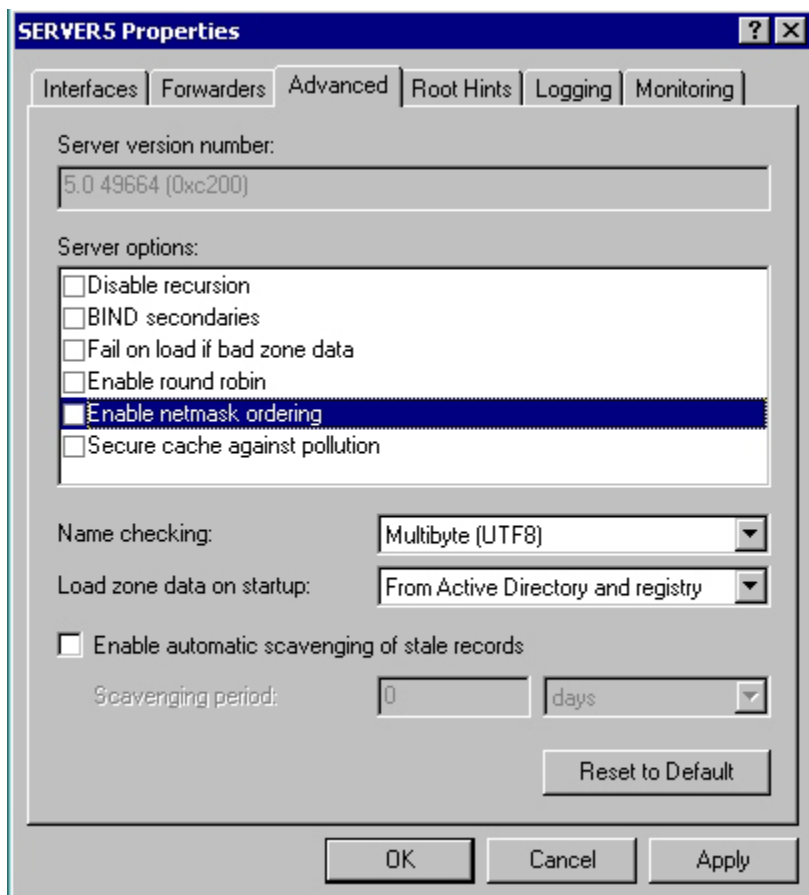
To answer, click the appropriate check box in the Advanced tab of the Properties dialog box.

Answer: In the Server options list, select the 'Bind Secondaries' check box.
Explanation: Bind secondaries determines whether to use fast transfer format when transferring a zone to DNS servers running legacy Berkeley Internet Name Domain (BIND) implementations. By default, all Windows-

based DNS servers use a fast zone transfer format, which uses compression and can include multiple records per TCP message during a connected transfer. This format is also compatible with more recent BIND-based DNS servers that run versions 4.9.4 and later. In this scenario the ISP's DNS server does not appear to support this, and Bind secondaries needs to be enabled.

QUESTION NO: 4
You are the administrator of TestKing's network. You configure a Windows 2000 Server computer as the DNS server for your network. You create both standard primary forward lookup and reverse lookup zones.

You discover that when you use the nslookup utility, you cannot resolve host names from IP addresses on your network. You also discover that when you run the Tracert.exe utility, you receive the following error message. "Unable to resolve target system name."

What should you do?

A. Configure the DNS to forward requests to an external DNS
B. Install a WINS server and configure DHCP to issue the IP address of the WINS server to all DHCP clients
C. Create PTR (pointer) records in your reverse lookup zone
D. Copy the systemroot\system32\dns\cache\samples\cache.dns to systemroot\system32\dns\cache\cache.dns

Answer: C
Explanation: Tracert is a utility that checks the route to a remote system. Tracert needs to resolve host names to IP addresses and IP addresses to host names to function. If tracert does not work it a very likely cause is that the reverse lookup mechanism does not work.
The NSLOOKUP command-line utility, use reverse lookup queries to report back host names.
A reverse lookup zone is created, but the reverse lookup zone is either not activated or there is missing PTR records in the reverse lookup zone.

Incorrect Answers:
A: This a reverse resolution problem. Using an external DNS server would not help.
B: WINS resolves NetBIOS names to IP address. WINS cannot solve problem with the reverse lookup zone.
D: Copying the systemroot\system32\dns\cache\samples\cache.dns to
         systemroot\system32\dns\cache\cache.dns would replace the root hints, but it would not fix the problem with the reverse lookups.

QUESTION NO: 5
You are the administrator of TestKing's network. Your Windows 2000 Server computer named Srv2 cannot communicate with your UNIX server named Srv1. Srv2 can communicate with other computers

on your network. **You try to ping Srv1, but you receive the following error message,** "Unknown host
Srv1".

**You create an A (host) record that has the correct name and IP address. However, when you try to ping
Srv1 again, you receive the same error message.**

What should you do to resolve this problem?

    A.   Restart the DNS server.
    B.   Clear the DNS Server Cache.
    C.   Run the **ipconfig /registerdns** command on Srv2.
    D.   Run the **ipconfig /flushdns** command on Srv2.

Answer: D.
Explanation: In this scenario there is a negative-cache entry in the DNS client resolver cache, which prevents
communication with Srv1. The command ipconfig/flushdns can be used to remove all entries in the DNS client
resolver cache and resets the DNS name cache. This will resolve the problem.

Incorrect Answers:
A: Restarting the DNS server will not reset the DNS client name cache.
B: The problem is at the client, not at the Server. The DNS client cache, not the DNS server cache, needs to
        be cleared.
C: The ipconfig /registerdns command refreshes all DHCP address leases and registers all related DNS
        names configured and used by the client computer. It will not remove the negative cache entry in the
        DNS client cache.

QUESTION NO: 6
**You are the administrator of TestKing's network. The network consists of one Windows 2000 domain.
All servers and client computers are running Windows 2000. To facilitate name resolution and client
access to resources on the servers, you have configured your DNS standard primary zone to include the
addresses of all of your servers. You later add three new member servers to your network. Users report
that they can find these servers in the directory but cannot access these servers.**

You want to resolve this problem. What should you do?

    A.   Convert the DNS standard primary zone to an Active Directory integrated zone
    B.   Create SRV (service) records for each new server in the DNS zone.
    C.   Set the **Allow Dynamic Updates** setting for the DNS standard primary zone to **Yes**
    D.   Set the **Allow Dynamic Updates** setting for the DNS standard primary zone to **Only Secure**
        Updates

Answer: C.
Explanation: The problem in this scenario is that the new servers are not allowed to dynamically register their own names in the DNS zone. Windows 2000 DNS server supports dynamic updates but the zone has to be configured to accept them. This can be configured from Administrative Tools by opening the DNS console, right click the zone, select Properties, select the General tab, enable Allow dynamic updates.

Incorrect Answers:
A: It is not necessary to convert the standard primary zone to an Active-integrated zone. Dynamic updates will allow the members servers to register in a standard primary zone.
B: The new servers are member servers and there is no mention of them doing any special services in the domain. It is not necessary to add SRV (service) records for them.
D: The DNS zone is a standard primary zone. The Only Secure Updates option only appears if the zone type is Active Directory-integrated.

QUESTION NO: 7
You are the administrator of a Windows 2000 network that consists of three subnets. For load-balancing purposes, each Web server on the network is configured to maintain exactly the same content as all the other web servers.

You want to configure your DNS server to allow users to type a host name in their browser to connect to Web server that is on the same subnet. The host name that all users type will be identical regardless of the subnet they are on.

How should you configure your DNS server?

    A.   On the primary DNS server, create three A (host) records that map the same host name to the IP address of the Web server on each subnet.
    B.   On the primary DNS server, create one A (host) record that is located on the same subnet as the DNS server.
          On the secondary DNS servers on the two remaining subnets, edit the zone file for the domain on each DNS server to include an A (host) record for the Web server on each subnet.
    C.   On the primary DNS server, create three A (host) records that map a different host name to the IP address of the Web server on each subnet.
    D.   On the primary DNS server, create one A (host) record for one Web server and two CNAME (canonical name) records for the remaining two Web servers.

Answer: A.
Explanation: This is Subnet Prioritization by mapping the same host name (A record) to three different IP addresses. If the resolver receives multiple A resource records from a DNS server, and some have IP addresses from networks to which the computer is directly connected to, the resolver orders those resource records first. This reduces network traffic across subnets by forcing computers to connect to network resources that are closer to them.

Incorrect Answers:
B: The secondary DNS zone contains a read-only replica of the primary DNS zone. Therefore we should not make changes to the zone at the secondary DNS servers.
C: We want the users to use only one host name, not a different one on each subnet.
D: A canonical name (CNAME) record enables us to associate more than one host name with an IP address. This is sometimes referred to as aliasing. But we want the users to use the same host name, not different aliases of it.

QUESTION NO: 8
You are the network administrator of Woodgrove Bank. Your network is configured as shown in the exhibit.
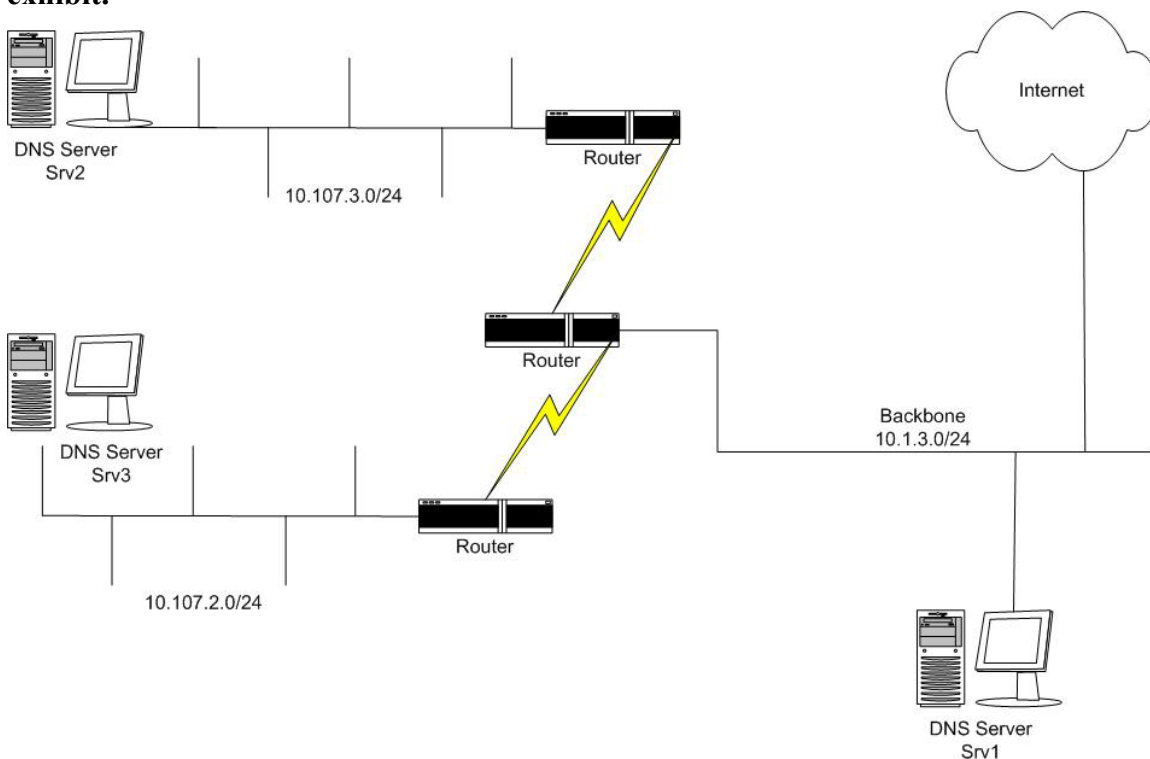
Srv2 and Srv3 are configured as caching-only servers. Both servers forward requests to Srv1. Srv1 is configured as the primary Server for the woodgrovebank.com domain.

Users on networks 10.107.2.0 and 10.107.3.0 frequently use an Internet application that gathers stock quotes from various servers on the woodgrovebank.com domain.

You want to reduce DNS network traffic. What should you do?

    A.   Increase the Time to Live (TTL) for the SOA (start of authority) record on Srv1.
    B.   Decrease the Time to Live (TTL) for the SOA (start of authority) record on Srv2 and Srv3.

C.   Set the **Server Optimization** option on Srv2 and Srv3 to **Maximize data throughput for network applications**.
D.   Increase the forward time-out seconds on Srv2 and Srv3.

Answer: A.
Explanation: The name server caches the query result for a specified amount of time; this is referred to as Time to Live (TTL). A longer TTL value will increase the time that records can be cached in the DNS caching only servers, thus decreasing DNS network traffic. The drawback is the risk of DNS name inconsistencies. The SOA (start of authority) record indicates the starting point or original point of authority for information stored in a zone. The SOA record is stored at the primary DNS server, SRV1, not at Srv2 and Srv3.

Incorrect Answers:
B: The SOA record is stored at the primary DNS server, SRV1, not at Srv2 and Srv3.
C: The server optimization option "Maximize Throughput for Network Applications" is selected instead of the default "Maximize Throughput for File Sharing" to avoid excessive paging (due to large file server cache) on servers that are used for network programs and services such as SQL Server. In this scenario we want to reduce DNS network traffic, not reduce paging.
D: The "Forward Time out" decides how long the DNS server, in this case Srv2 and Srv3, will repeatedly query the forwarder, in this case Srv1, until the "Forward Time Out" time is reached, or it gets an answer. This setting will not decrease any DNS traffic.

QUESTION NO: 9
You are the administrator of Windows 2000 network. Your network has one primary internal DNS server and one primary external DNS server.

You network has three secondary DNS servers that transfer zone information from the primary external DNS server. The secondary DNS servers are installed on two Windows 2000 Server computers and one Windows NT 4.0 computer.

The primary external DNS server is used to host records for TestKing's Web and mail servers. It has only a limited number of resource records in its zone file. The Web server and the mail server have static IP addresses.

When you monitor the secondary DNS servers by using System Monitor, you notice a high number of hits when monitoring the counter DNS: Zone Transfer SOA Requests Sent. You want to minimize the bandwidth that is required for the traffic.

What should you do? (Choose two)

A.   Upgrade the Windows NT Server 4.0 computer that is hosting the secondary DNS server to a Windows 2000 Server computer.

B.   Configure that notify list on the primary external DNS server to notify the secondary DNS server when there are changes to be replicated.
C.   Reconfigure the primary external DNS server so that it does not allow dynamic updates.
D.   Increase the value of the Refresh interval in the SOA (start of authority) record.
E.   Decrease the value of the Refresh interval in the SOA (start of authority) record.

Answer: B, D.
Explanation: The value of the refresh interval in the SOA (start of authority) record, which has a default value is 15 minutes, decides how often the destination server should request to renew the zone. By increasing this value less zone transfers would occur. However, the danger of increasing the refresh interval of the SOA is DNS inconsistencies in the network. Configuring the notify list on the external DNS server to notify the secondary server, will force changes to be transferred and thus avoiding inconsistencies.

Incorrect Answers:
A: Upgrading the Windows NT 4.0 secondary DNS server to Windows 2000 will not decrease network bandwidth requirements; they use the same kind of zone transfers. By upgrading to Windows 2000 and changing the zone type to Active Directory-integrated the bandwidth would decrease thanks to incremental zone transfers.
C: By disallowing dynamic updates on the external server we will prevent clients from registering themselves in DNS. This will however not decrease bandwidth.
E: By decreasing refresh interval in the SOA zone transfers would occur more frequently. It should be increased instead.

QUESTION NO: 10
You are the network administrator for the branch office of a large company. Your network is connected to the company network by means of a Windows 2000 Routing and Remote Access two-way demand dial connection over ISDN. To reduce costs, the ISDN links should only be used once each day to transfer sales information to or from the main office. This transfer should occur during nonbusiness hours.

You discover that several times a day an ISDN link is initiated between the networks. You analyze the traffic and discover that it is composed of router announcement broadcasts.

Which actions should you take to prevent the link from being used during business hours? (Choose Two)

A.   Schedule the demand-dial interface to dial only during specific hours.
B.   Schedule the demand-dial interface to accept only inbound connections during specified hours.
C.   Create the demand-dial filter on the demand dial interface.
D.   Enable dynamic routing on the demand-dial interface.
E.   Create a remote access policy to access the port used by router broadcasts.
F.   Create a remote access policy to restrict access to only the specific users who transfer information across the link.

Answer: A, C.
Explanation: Demand-dial filters control what traffic will initiate the demand-dial link. Filters can be set to permit or deny specific source or destination IP addresses, ports, or protocols. Further control is offered through the use of time-of-day restrictions. Even though the demand-dial filter requirements are met, if the time of day is restricted by the configuration of dial-out hours, the router will not dial.

Reference: Windows 2000 Server documentation, Demand-dial routing design considerations

Incorrect Answers:
B: The demand-dial interface is only used for outbound traffic and cannot be configured to accept only inbound connections during specified hours.
D: We cannot use dynamic routing on demand-dial interfaces.
E: Remote access policies are used to determine whether to accept or reject connection attempts, not to specify ports.
F: In this scenario there is no requirement to restrict access to specific users. Instead use demand-dial filters and dial-out hours to restrict access.

QUESTION NO: 11
You are the desktop administrator of your company. You are responsible for ensuring that TestKing's Windows 2000 Professional client computers have connectivity to the network and the Internet. All client computers use DHCP for their TCP/IP configuration.

The network administrators install a new T1 line and router for Internet access. This router must only be used by administrative staff. You want to configure the administrative staff's client computers to use this new router. You want to ensure that nonadministrative staff users cannot gain access to the Internet through this router. You want to ensure that each targeted client computer will only need to be configured once.

What should you do to achieve these goals?

A.   At each administrative client computer, use the **route add -f** command to enter the new router information.
B.   At each administrative client computer, use the **route add -p** command to enter the new router information.
C.   Enable the **Perform Router Discovery** option in the scope options for DHCP.
D.   Enter the new router's address in the **Router Solicitation Address** option in the scope options for DHCP.

Answer: B.
Explanation: By default, routes are not preserved when the computer is restarted. However, by using the ROUTE ADD –p command to add the appropriate route at the administrative client computers, the route is

made persistent, even after system reboots. Furthermore, by changing the default gateway, that is entering the router information, the new router would be used by the client. These steps will enable the client computers to gain Internet access through the new router needs to be done once only.

Incorrect Answers:
A: The –f switch clears all routes, which is not desirable. We should instead make the routes persistent.
C: Router discovery option of DHCP is used to configure a default Gateway (router). This setting will be applied to all computers, even the nonadministrative computers, which would allow ordinary users to access Internet.
D: This setting would apply to all computers, which makes it impossible to give some users (administrators) Internet access and prevent outer users from gaining access to Internet.

QUESTION NO: 12
You are the network administrator for a branch office of a large company. Your network is connected to the company network by means of a Windows 2000 Routing and Remote Access two-way demand-dial connection over ISDN. In addition to e-mail and application traffic, sensitive company data is transferred across this connection.

You want to accomplish the following goals:

- **All data transmitted over the connection will be secured.**
- **Rouge routers will be prevented from exchanging router information with either router.**
- **Both routers in the connection will be able to validate each other.**
- **Both routers in the connection will maintain up-to-date routing tables.**
- **Traffic over the demand-dial link during peak business hours will be minimized.**

You take the following actions:

- **Install a Certificate Services server at the main office.**
- **Enable EAP-TLS as the authentication protocol on both Routing and Remote Access servers.**
- **Enable RIP version 2 on the demand dial interfaces.**

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

A. All data transmitted over the connection is secure.
B. Rouge routers are prevented from exchanging router information with either router.
C. Both routers in the connection are able to validate each other.
D. Both routers in the connection are maintaining up-to-date routing tables.
E. Traffic over the demand-dial link during peak business hours is minimized.

Answer: A, C, D.

Explanation: We have enable EAP-TLS as the authentication protocol on both routing and remote access servers. The EAP (Extensible Authentication Protocol) supplies secure mutual authentication, therefore the routers would be able to validate each other in a secure way.

EAP-Transport Level Security (EAP-TLS) supplies data encryption as well, which makes the transmitted data secure. We have enabled RIP V2, which is used to keep the routing tables up-to-date by frequent broadcasts.

Incorrect Answers:
B: RIP version 2 is able to detect Rogue Routers but we must enable this detection.
E: In order to minimize traffic during peak business hours we would have to configure a Remote Access Policy.

QUESTION NO: 13
You are the administrator of TestKing's network. The network consists of two locations named East and West. Each location contains a Windows 2000 Server computer and 45 Windows 2000 Professional computers. The two servers are Windows 2000-based routers. The two routers are not connected to each other, but both are connected to a third router named Central. The central router is administered by a different company.

The network is shown in the exhibit.
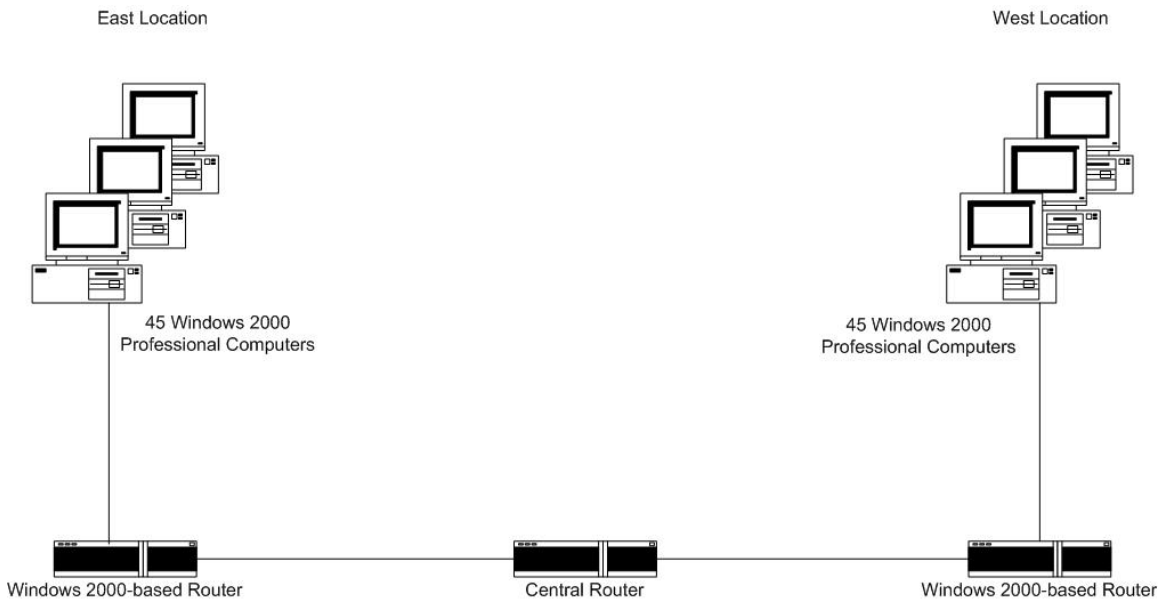
Users in the both locations want to provide multicast-based datacasting of information to the other location.

You add the Internet Group Management Protocol (IGMP) to both the servers. However, the Central router does not support multicast forwarding or routing.

How should you configure the network to allow IP multicast traffic to pass between the east and the west locations?

    A.   On both servers, create a static route. Use the IP address of the other server as a gateway.

    B.   On both servers, assign the interface for the Central router to the IGMP routing protocol.
           Run these interfaces in IGMP proxy mode.

    C.   Create an IP-in-IP interface between the two servers.
           Assign the IP-in-IP interface to the IGMP routing protocol.
           Run the interface in the IGMP proxy mode.

    D.   Add the RIP for IP routing protocol to both servers.
           Assign the interface for the Central router to the RIP routing protocol.
           Configure the servers to be unicast neighbors of each other.

Answer: C.
Explanation: By creating IP-in-IP interface between the two routers, assigning the IGMP routing protocol to the interface and running the interface in IGMP proxy mode the routers will have a multicast tunnel that works even though the central router supports neither multicast routing nor forwarding.
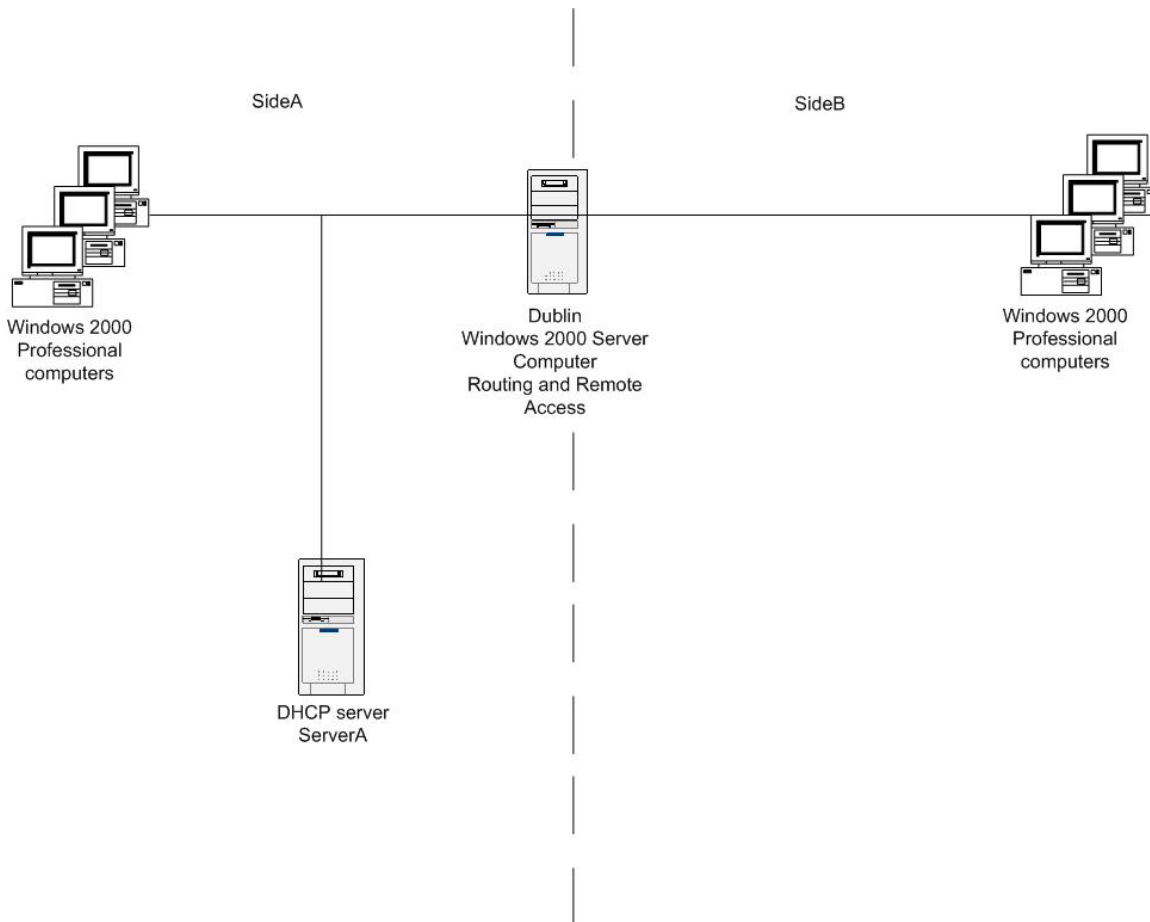
Incorrect Answers:
A: The central router does not support multicast forwarding therefore an IGMP proxy mode has to be used.
B: The central router does not support multicast routing therefore an IP-in-IP tunnel must be created.
D: The central router does not support multicast routing therefore an IP-in-IP tunnel must be created.

QUESTION NO: 14
You are the administrator of Windows 2000 network. The network contains a Windows 2000 Server computer named Dublin. Dublin has two network interfaces named SideA and SideB. Routing and Remote Access is enabled as a router on Dublin.

Only the network segment connected to the SideA interface has a DHCP server. The DHCP server is a Windows 2000 Server named ServerA.

The network is shown in the exhibit. .

SideA   SideB

Windows 2000
Professional
computers

Dublin
Windows 2000 Server
Computer
Routing and Remote
Access

Windows 2000
Professional
computers

DHCP server
ServerA

You want to allow computers on segment connected to the SideB interface to receive IP addresses from ServerA.

How should you configure Dublin to accomplish this goal? (Choose all that apply)

A.   Create an IP tunnel to connect the SideA interface to the SideB interface.
B.   Create a static route to the IP address of the SideB interface.
C.   Configure the DHCP Relay Agent routing protocol to run the SideA interface.
D.   Configure the DHCP Relay Agent routing protocol to run the SideB interface.
E.   Configure the DHCP Relay Agent routing protocol to use the IP address of the DHCP server as the server address.
F.   Configure the DHCP Relay Agent routing protocol to use the port number of the DHCP server.

Answer: D, E.
Explanation: In this scenario the clients on SideB are not able to receive DHCP information from the DHCP server on SideA. In order to enable this, a DHCP relay agent must be configured on the SideB LAN interface on the Router Dublin. This is done by adding the SideB interface to the DHCP Relay Agent IP routing protocol.

The DHCP Relay Agent protocol must also be configured with the IP address of a DHCP server, in this case the IP address of ServerA.

Incorrect Answers:
A: IP tunnels are used between different computers, not between different LAN interfaces on a Router.
B: A static router between the SideA and SideB interfaces will not enable communication between the client on segment B and the DHCP server.
C: DHCP Relay Agent routing protocol must be configured on the interface to the segment which has no DHCP server. It must thus be configured on the SideB interface not the SideA interface.
F: The DHCP Relay Agent protocol must also be configured with the IP address of a DHCP server, not the port number of the DHCP server.

QUESTION NO: 15
You are the administrator of a Windows 2000 network for your company. The company has a main office in Atlanta and branch office locations in Boston, Chicago and Dallas. The three branch office locations are connected to the Atlanta location by means of Windows 2000-based routers. All four locations have a Windows 2000-based DHCP Server.

The network is shown in the exhibit.
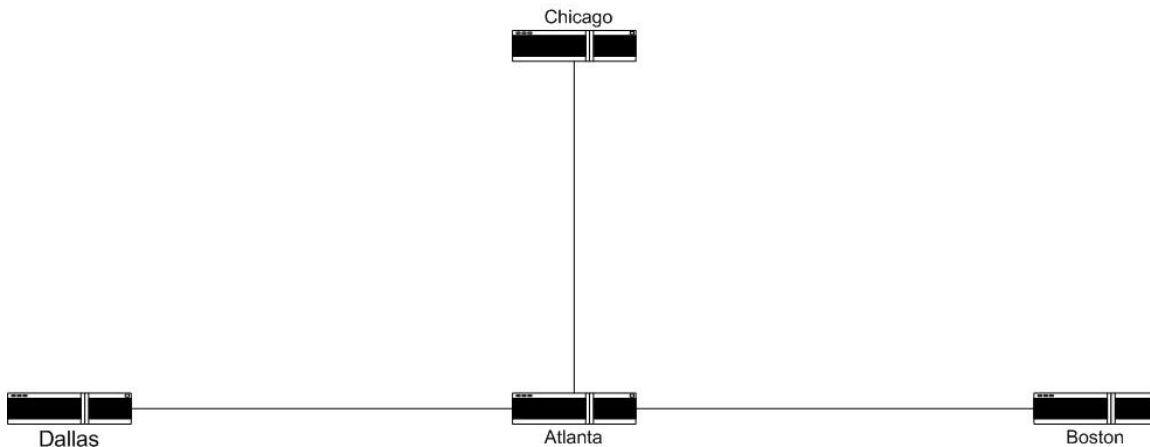
Each Friday, the Atlanta location hosts a multicast video presentation that is broadcast to all four locations. The Atlanta location also frequently hosts multicasting video presentation intended for the sales staff in the Atlanta and Boston locations only. You want to ensure that these sales staff multicasting video presentations are not sent to the Chicago and Dallas locations.

You assign specific IP multicast addresses for use with the sales staff multicasting video presentations.

How should you configure the network to prevent the forwarding of the sales staff multicasting video presentations to the Chicago and Dallas locations?

Leading the way in IT testing and certification tools, www.testking.com

A.   Configure a multicast scope boundary for the sales IP multicast addresses on the Chicago and Dallas interfaces of the Atlanta router.
B.   Configure the DHCP servers to provide a multicast scope for the sales IP multicast addresses. At the Chicago and Dallas locations, configure the scope to use a Time to Live (TTL) of 0. At the Atlanta and Boston locations, use the default multicast TTL.
C.   Configure the network connections to the Chicago and Dallas locations to use TCP/IP filtering. Do not permit network traffic that has IP multicast addresses.
D.   On the central router, configure a static route for the sales IP multicast addresses. Use the router IP address at the Boston location as the gateway for this static route.

Answer: A.
Explanation: Multicast boundaries are administrative barriers to the forwarding of IP multicast traffic. Without boundaries, an IP multicast router would forward all appropriate IP multicast traffic. In this scenario we want to prevent multicasting on the Chicago and Dallas interfaces on the Atlanta router. This can be accomplished by adding the sales multicasting IP addresses to these interfaces.

Incorrect Answers:
B: Multicast boundaries are configured in the RRAS console, not by configuring scopes with the DHCP console.
C: TCP/IP filtering cannot be used to prevent multicasting on particular interfaces. Multicast boundaries must be configured and used on those interfaces.
D: Multicast boundaries, not static routes, are used to prevent multicasting on specific router interfaces.

QUESTION NO: 16
You are the administrator of a Windows 2000 network. Some of the members of TestKing's graphics department use Macintosh computers and are not using Internet Explorer as their browser. These users inform you that they cannot request valid user certificate from your Enterprise Certificate Authority (CA). You want to make it possible for these users to request certificates by using Web-based enrollment.

What should you do?

A.   In the Internet Information Services (IIS) console, access the properties for the CertSrv virtual directory. On the **Directory Security** tab, set the authentication type to **Basic Authentication**.
B.   In the Policy Settings container in the CA console for your CA, add a new Enrollment Agent certificate.
C.   Edit the ACL on the user certificate template to grant the graphics department users enroll access.
D.   In the Internet Information Services (IIS) console, access the properties for the CertSrv virtual directory. On the **Directory Security** tab, set the authentication type to **Integrated Windows Authentication**.

Answer: A.

Explanation: IIS has four levels of authentication: anonymous access, which grants anyone access; basic authentication, which sends passwords over the connection in clear text; integrated Windows authentication, which uses Kerberos V5 and can only be used by Windows clients; and digest authentication, which is the best choice for publishing information on a server over the Internet and through firewalls. In this scenario there is a need to relax security so that the Macintosh users will be able to request certificates by using web-based enrollment. By setting the authentication type to Basic Authentication most browsers will be able to connect to the IIS server.

Incorrect Answers:
B: A new enrollment agent certificate is not needed. The Windows users are able to use the current one and so will the Macintosh users when the authentication type is changed to Basic Authentication.
C: It is not necessary to change the ACL on the user certificate template for the users in the graphics department. The Windows users in the graphics department have no problem with IIS.
D: Integrated Windows authentication uses Kerberos V5 and can only be used by Windows clients.

QUESTION NO: 17
You are the administrator of a Web server hosted on the Internet that is running on a Windows 2000 Server computer. TestKing's Web developers have developed applications that download ActiveX controls automatically to your customers' browsers. You discover that the default security settings on your customers' browsers are preventing the ActiveX controls from being downloaded automatically. You want to facilitate the downloading of ActiveX controls from your Web server to the Internet clients.

What should you do?

  A.   Install an Enterprise Subordinate Certificate Authority (CA) that uses a commercial CA as the parent.
          Create a policy on the CA that allows the Web developers to request a certificate for code signing.
  B.   Install an Enterprise Certificate Authority (CA).
          Create a policy on the CA that allows the Web developers to request a certificate for trust list signing.
  C.   Install an Enterprise Subordinate Certificate Authority (CA) that uses a commercial CA as the parent.
          Create a policy on the CA that allows the Web developers to request a certificate for trust list signing
  D.   Install an Enterprise Certificate Authority (CA).
          Create a policy on the CA that allows the Web developers to request a certificate for code signing

Answer: A
Explanation: A commercial Certificate Authority is needed since external clients on the Internet will use the Active X controls. The web developers need to sign their Active X controls with code signing certificates.

Incorrect Answers:

B: An Enterprise Certificate Authority is used within a Windows Domain and would not be accessible by Internet users. The customers are external and would not be able to access an Enterprise Certificate Authority (CA). A commercial Certificate Authority is needed.

C: Trust list signing is a mechanism for allowing an administrator to specify a collection of trusted CAs. Trust list signing cannot be used to enable downloading of Active X controls.

D: An Enterprise Certificate Authority is used within a Windows Domain and would not be accessible by Internet users. The customers are external and would not be able to access an Enterprise Certificate Authority (CA). A commercial Certificate Authority is needed.

QUESTION NO: 18
You are the administrator of TestKing's network. You are configuring your users' portable computer to allow users to connect to the company network by using routing and remote access. You test the portable computers on the LAN and verify that they can successfully connect to sources on the company network by name.

When to test the connection through remote access, all the portable computers can successfully connect, but they cannot access files on the computers on different segments by using the computer name.

What should you do to resolve the problem?

    A.   Set the authentication method to **Allow remote systems to connect without authentication**.
    B.   Enable the computer account for each portable computer.
    C.   Change the computer name on each portable computer.
    D.   Install the DHCP relay agent on the remote access server.

Answer: D
Explanation: The DHCP relay agent must be installed on the Routing and Remote Access (RRAS) server. The DHCP relay agent will allow communication between the DHCP server and the RAS clients. In particular the RAS clients would be given the Default Gateway that has been configured for the scope at the DHCP server.

Incorrect Answers:
A: The RAS clients have already connected successfully. The problem is the Default Gateway setting of the clients not the authentication method at the RRAS server.
B: It is not necessary to enable the computer accounts. The remote users already have access to the network.
C: It is not necessary rename the computers. The remote users already have access to the network.

QUESTION NO: 19
You are the administrator of a Windows 2000 domain. The domain has a Windows 2000 member server computer named Delta. Routing and Remote Access is enabled for remote access on Delta. The domain is

in native mode. For all user accounts, the delta-in permission is set to control access through remote access policies.

You want to allow all users in the domain to dial in during the workday. You also want to allow only members of the global security group named Support Staff to be able to dial in between 6:00 P.M. and 8:00A.M. However, you do not want to allow the Support Staff members to be able to dial in when the log files are made each day between 7:00A.M. and 8:00A.M.

You create four remote access policies on Delta as shown in the following table.

<u>Name</u>	Condition	Permission	Profile
Domain users all policy	Windows-group=Domain users	Access	(default)
Support staff all policy	Windows-group=Support staff	Access	(default)
Domain users 6-8 policy	Day-and-Time=6P.M-8A.M Windows-group=Domain users	Deny	(default)
Support staff 7-8 policy	Day-and-Time=7A.M-8P.M Windows-group=Support staff	Deny	(default)

To specify the appropriate access control for Delta, click the Select and Place button, and then drag the remote access policies and place them in the correct order.

Select and Place

Order	Policies
	Select from these items

Order

1 Place policy here

2 Place policy here

3 Place policy here

4 Place policy here

Policies

Select from these items

Domain Users all policy

Support staff all policy

Domain users 6-8 policy

Support staff 7-8 policy

Answer:

Order		Policies
		Select from these items
1	Support staff 7-8 policy	
2	Support staff all policy	
3	Domain users 6-8 policy	
4	Domain Users all policy	
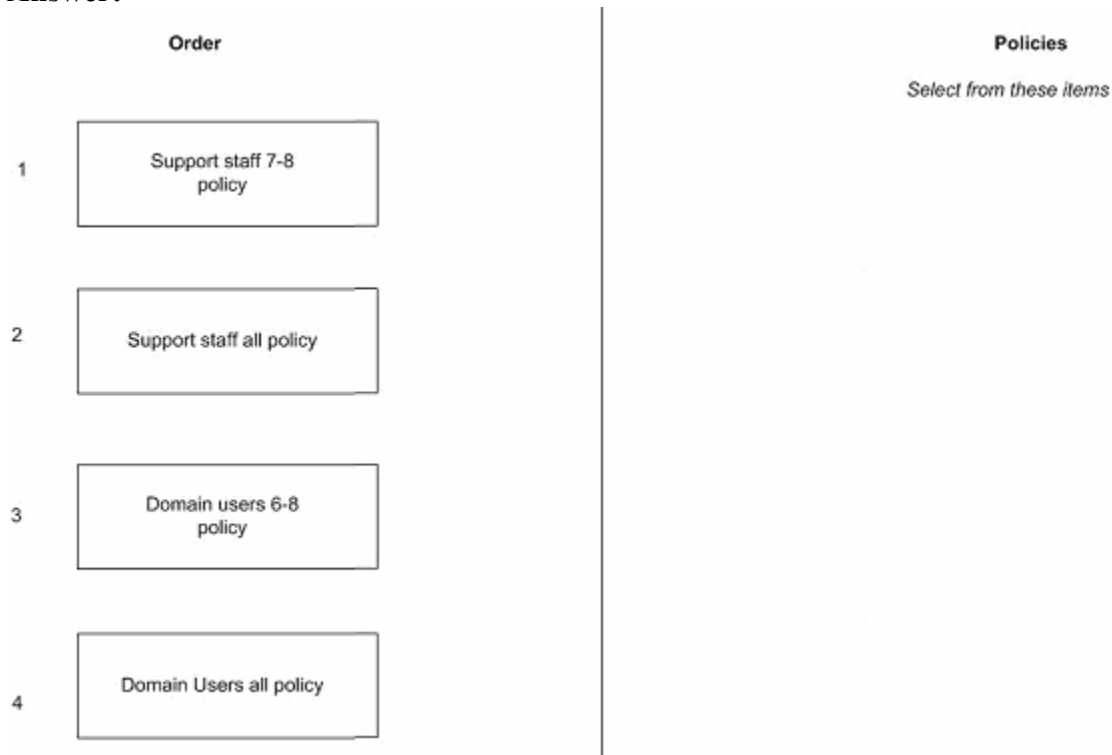
1. Support staff 7-8 Deny
2. Support staff all
3. Domain users' 6-8 Deny
4. Domain users all

Explanation: The Remote Access Policies are applied in order. The first policy which meets the conditions is applied. Only one policy can be applied.
Support staff policies must be applied before the Domain users policies, since the staff members also are Domain users, and staff members need access 5-7 A.M.
The Deny policies must be applied before the allow policies. If not the Deny policies would never be applied.

QUESTION NO: 20
You are the administrator of TestKing's network. To facilitate connections for remote administration, you install Routing and Remote Access on a Windows 2000 domain controller.
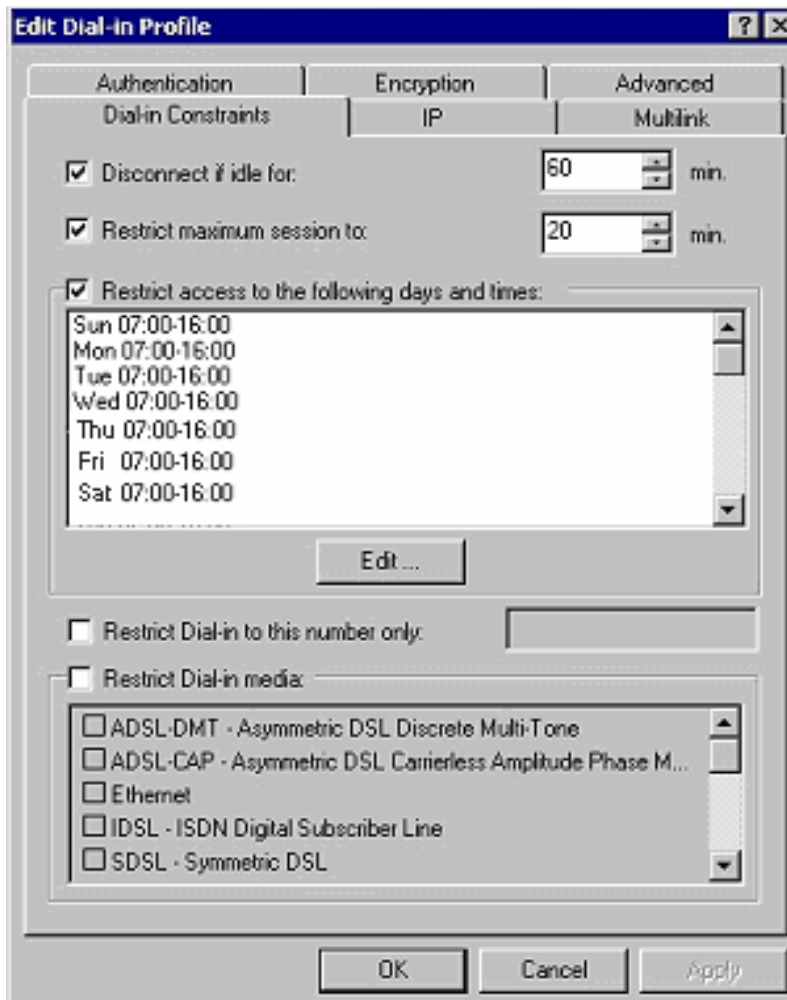
You want to accomplish the following goals:

- **Only administrators will have dial-up access.**
- **Dial-up connections will be accepted only from 4.00 p.m. to 7.00 a.m.**
- **Connections will be forcibly disconnected after 20 minutes of inactivity**
- **All connections will encrypt all communications**

- **Connections will be limited to one hour**

You take the following actions:

- **Set the level or levels of encryption to No Encryption and Basic.**
- **Add Domain Admins to the Windows Group Policy condition.**
- **Configure the rest of the remote access policy as shown in the exhibit**

```
Edit Dial-in Profile                                    ? ×

   Authentication   |      Encryption     |      Advanced
     Dial-in Constraints    |      IP       |      Multilink

   ☑ Disconnect if idle for:          [60]  ↕  min.

   ☑ Restrict maximum session to:     [20]  ↕  min.

   ☑ Restrict access to the following days and times:
   ┌──────────────────────────────────────┐▲
   │ Sun 07:00-16:00                       │█
   │ Mon 07:00-16:00                       │█
   │ Tue 07:00-16:00                       │█
   │ Wed 07:00-16:00                       │
   │ Thu 07:00-16:00                       │
   │ Fri  07:00-16:00                      │
   │ Sat 07:00-16:00                       │
   └──────────────────────────────────────┘▼

                    [   Edit ...   ]

   ☐ Restrict Dial-in to this number only:  [                ]

   ┌─ ☐ Restrict Dial-in media: ─────────────────────┐
   │ ☐ ADSL-DMT - Asymmetric DSL Discrete Multi-Tone │▲
   │ ☐ ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase M... │█
   │ ☐ Ethernet                                      │
   │ ☐ IDSL - ISDN Digital Subscriber Line           │
   │ ☐ SDSL - Symmetric DSL                          │▼
   └─────────────────────────────────────────────────┘

          [   OK   ]   [  Cancel  ]   [  Apply  ]
```

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

A.   Only administrators have dial-up access
B.   Dial-up connections are accepted only between 4:00 PM and 7:00 A.M
C.   Connections are forcibly disconnected after 20 minutes of inactivity
D.   All connections encrypt all communication
E.   Connections are limited to one hour

Answer: A, C
Explanation: The exhibit indicates that the default remote access policy (RAP) has been changed. This is the only RAP used. By adding the Domain Admins to the Windows Group Policy condition only the administrators have dial-up access. Furthermore, the maximum session is set to 20 minutes, therefore after 20 minutes of being connected, including being idle for 20 minutes, a forced disconnection will occur.

Incorrect Answers:
B: Dial-up connections are configured to restrict access to between 7:00 am and 4:00 pm as is shown in the exhibit. Therefore connections will not be accepted between 4:00pm and 7:00 am the following morning.
D: Some connections might be unencrypted since Basic and No encryption is allowed.
E: Although the idle time limit is one hour, the session time is limited to 20 minutes, therefore connections are limited to 20 minutes, not one hour.

QUESTION NO: 21
You are the administrator of TestKing's Routing and Remote Access servers. TestKing's administrators are able to dial in to the company's network to perform remote monitoring and administration. This remote monitoring and administration requires an excessive amount of network bandwidth. You want to allow only administrators to use multiple phone lines, and you want to limit all other users to a single phone line.

You want to configure multiple phone-line network connections to adapt to changing bandwidth conditions. When the phone lines fall below 50 percent capacity, you want to reduce the number of phone lines utilized. You also want to allow all users the ability to connect to the network by Routing and Remote Access. No default remote access policies currently exist.

What should you do? (Choose three)

A. Create one remote access policy on the Routing and Remote Access server.
B. Create two remote access policies on the Routing and Remote Access server.
C. Allow Multilink.
D. Decrease the maximum number of ports used by the Routing and Remote Access server.
E. Select the **Require Bandwidth Allocation Protocol (BAP) for the Dynamic Multilink Requests** check box.
F. Increase the maximum number of dial-up sessions.

Answer: B, C, E
Explanation: No default remote access policy exists in Windows 2000. We need to create two Remote Access Policies (RAPs); one which applies to the administrators and on which applies to the ordinary users. Multilink has to be allowed for the Administrator RAP.
The Routing and Remote Access console is then used to enable multilink and to enable the Bandwidth allocation Protocol.

Incorrect Answers:
A: Two RAPs have to be created, not one. One should be created for the Administrators and another for the Users.
D: Decreasing the number of ports used on the Routing and Remote Access server will decrease the number of simultaneous connections. This is not in keeping with the requirements set out in this scenario.
F: Multilink has to be enabled, the number of dial-up sessions does not have to be increased.

QUESTION NO: 22
You are the administrator of TestKing's network. Your company has branch offices in New York and Paris. Because each branch office will support its own Routing and Remote Access server, you implement a Remote Authentication Dial-In User Service (RADIUS) server to centralize administration.

You remove the default remote access policy. You need to implement one company policy that requires all dial-up communications to use 40-bit encryption. You want to configure your network to require secure communications by using the least amount of administrative effort.

What should you do? (Choose two)

A. Create one remote access policy on each Routing and Remote Access server.
B. Create one remote access policy on the RADIUS server.
C. Set encryption to **Basic** in the remote access policy or policies.
D. Set encryption to **Strong** in the remote access policy or policies.
E. Enable the Secure Server IPSec policy on the RADIUS server.
F. Enable the Server IPSec policy on the RADIUS server.

Answer: B, C.
Explanation: IAS, Microsoft's implementation of RADIUS server, is used to centralize administration, authentication, and authorization of RAS. Remote Access Policies is included in this centralization. Furthermore, there are 3 levels of encryption on dial-up connections: basic, strong and strongest. Basic is 40-bit encryption and is used on older Windows systems. Strong is 56-bit encryption and strongest is 128-bit encryption. Strongest is only used inside North America because of legal issues.

Incorrect Answers:
A: Only one remote access policy at the RADIUS server has to be created, not one on each RRAS server.
D: If encryption were set to Strong in a remote access policy, 56-bit encryption would be used, this would not be compatible with older Windows systems. In this scenario 40-bit encryption is required.
E: By enabling the Secure Server (Require security) IPSec policy at the Radius server, any clients, including the Routing and Remote Access servers, which connect to this server must be IPSec-aware. They are not in this scenario.
F: Enabling the Server (Request security) IPSec policy at the Radius server, would still allow unencrypted communication initiated from a client who is not IPSec.

QUESTION NO: 23
You are the administrator of TestKing's network. You are configuring remote access services in your Windows 2000 domain to allow mobile users to access network resources. You want the inbound client connections to receive IP address administrator option configurations for the client computers.

Users report that they cannot access network resources by using the server name or by searching Active Directory. You investigate and find that when you connect to the remote access server, your client computer is receiving its IP address configuration but none of the DHCP options. Internal client computers are not experiencing this problem.

What should you do to resolve this problem?

    A.   Enable IP routing in the remote access Server's **Properties** dialog box.
    B.   Disable IP routing in the remote access Server's **Properties** dialog box.
    C.   Configure a static address pool on the remote access Server.
    D.   Configure the remote access server to act as a DHCP Relay Agent.

Answer: D
Explanation: In this scenario the mobile users receive their IP configurations from the Remote Access Server, but they are not able to receive any DHCP options. In order to enable this, a DHCP relay agent must be configured on the Remote Access server. This will allow DHCPINFORM, which are used to obtain Windows Internet Name Service (WINS) and Domain Name System (DNS) addresses, domain name, Default Gateway or other DHCP options originating from the DHCP server, to reach the mobile clients.

Incorrect Answers:
A: The mobile clients are able to connect to Remote Access Server. Therefore this is not a communication problem. Therefore enabling IP routing will not solve the problem.
B: The mobile clients are able to connect to Remote Access Server. Therefore this is not a communication problem. Therefore disabling IP routing will not solve the problem.
C: The mobile clients receive the correct IP configurations from the Remote Access Server. Therefore it is not necessary to create a static address pool on the remote access Server.

QUESTION NO: 24
You are the administrator of a Windows 2000 domain named contoso.com. The domain has a Windows 2000 member server computer named Ras1 and a Windows 2000-based DHCP server computer named Dora. Routing and Remote Access is enabled for access on Ras1. The network has two DNS servers that use IP addresses of 10.1.5.2 and 10.1.5.3.

Ras1 has configured to use DHCP to assign IP addresses to the remote access client computers.

The configuration of the scope options on the DHCP server is shown in the following Windows.
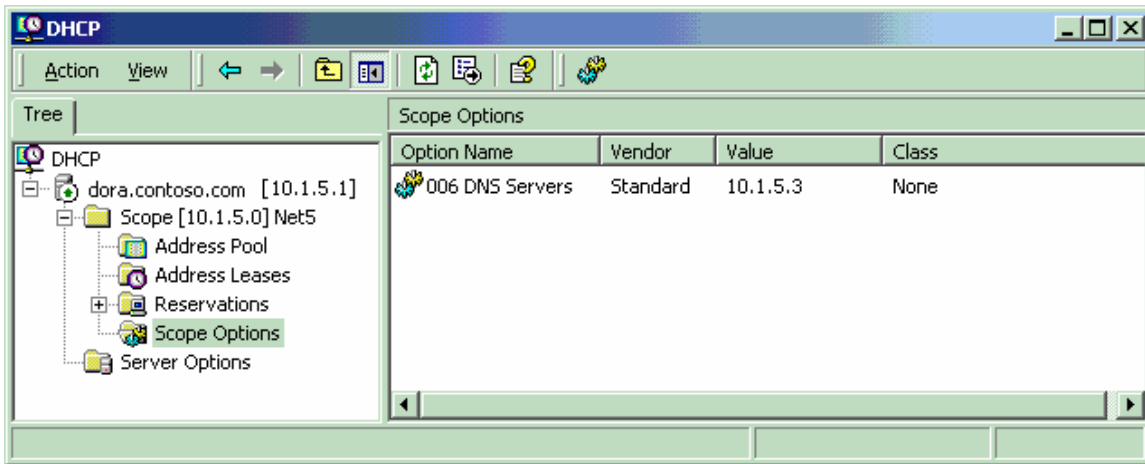
The DHCP scope does not have any client computer reservations.

When remote access client computers dial into Ras1, they receive an IP address form the DHCP scope range, but they do not receive the DNS address configured in the DHCP scope. Instead, the remote access client computers receive a DNS server address of 10.1.5.2.

You want the remote access client computers to receive the DNS option from the DHCP server.

How should you configure the network to accomplish this goal?

A.   Configure the remote access client computers to enable DHCP on the dial-up connection.
B.   Configure Ras1to use Windows Authentication.
C.   Install and configure the DHCP Relay Agent routing protocol on the Internet interface of Ras1.
D.   On the DHCP server, configure the DNS scope option of 10.1.5.3 for the Default Routing and Remote access user class.

Answer: C
Explanation: In this scenario, the remote clients are receiving the correct DNS server address, as it was specified in the scope. However, they are not able to receive DHCPINFORM packets from the DHCP server on Dora. In order to enable this, a DHCP relay agent must be configured on Internet interface of Ras1. This is done by adding the SideB interface to the DHCP Relay Agent IP routing protocol. The DHCP Relay Agent protocol must also be configured with the IP address of a DHCP server, in this case the IP address of ServerA.

Incorrect Answers:
A: DHCP cannot be configured on a dial-up connection.
B: This is a DCHP problem, not an authentication problem. The RAS clients can perform remote access, but they are configured with the incorrect DNS server.

Leading the way in IT testing and certification tools, *www.testking.com*

D: The exhibit indicates that the correct DNS scope option of 10.1.5.3 has already been defined. There is also no default routing and remote access user class.

QUESTION NO: 25
You are the administrator of a Windows 2000 domain. The domain has a Windows 2000 member server computer named Ras5. Routing and Remote Access is enabled for remote access on Ras5. The domain also has a Windows NT 4.0 member server computer named Ras4. Ras4 is running Remote Access Service (RAS). The domain is in mixed mode.

Users in the domain use Windows 2000 Professional computers to dial in to the network through Ras4 or Ras5. However, Ras4 is not able to validate remote access credentials of domain accounts.

How should you configure the network to enable the Windows NT 4.0 Ras4 member server computer to validate remote access domain users?

A. Change the domain from mixed mode to native mode.
B. Add the Ras4 computer account to the RAS and IAS Servers group.
C. Add the Everyone group to the Pre-Windows 2000 Compatible Access group.
D. Create a remote access policy that has the Ras4 computer account as a condition. Grant remote access permission if the condition matches the properties of the dial-in attempt.

Answer: C
Explanation: The Pre-Windows 2000 Compatible Access is a backward compatibility group which allows read access on all users and groups in the domain. In this the NT 4.0 RAS Server Ras4 needs to access the user accounts of the domain. This is done by adding the Everyone group to the Pre-Windows 2000 Compatible Access group. We can verify that the Everyone group is added to the Pre-Windows 2000 Compatible Access group with the net localgroup 'Pre-Windows 2000 Compatible Access' command. If not, we can issue the net localgroup 'Pre-Windows 2000 Compatible Access' everyone /add command on a domain controller computer and then restart the domain controller computer.

Incorrect Answers:
A: Changing to native mode is not required and would not address the problem.
B: The Windows NT 4.0 Ras server will not be able access properties of user account by adding it to any group. The Everyone group has to be added to the Pre-Windows 2000 Compatible Access group.
D: Creating a new remote access policy will not enable the NT 4.0 RAS server to access the properties of the user accounts of the domain.

QUESTION NO: 26
You are the administrator of TestKing's network, which consists of a single subnet. It includes 50 Windows 2000 Professional computers and four Windows 2000 server computers. One of these servers

runs DNS. The DNS server is configured to allow dynamic updates. All client computers and server are configured with static IP addresses and with the address of the DNS server.

You add two UNIX database servers named DB1 and DB2 to the network. From your client computer, you can ping both servers by using their IP addresses. However, when you try to run ping either server by name, you receive the following error message: "Unknown host".
You need to ensure that you can ping DB1 and DB2 by name. Which two actions should you perform? (Each correct answer presents part of the solution. choose two)

    A.   Add A (host) records to the DNS server for DB1 and DB2
    B.   Add SRV (service) records to the DNS server for DB1 and DB2
    C.   Disable dynamic updates on the DNS Server
    D.   Run the ipconfig/flushdns command on your client computer
    E.   Clear the DNS server cache

Answer: A, D
Explanation: To be able to ping a resource with a name, a forward lookup must be successful. Forward lookups uses Host (A) records. Host records for the two databases servers has to be added at the DNS Server. Then the DNS client resolver cache has to cleared, since a negative cache entry is preventing communication. The command ipconfig/flushdns removes all entries and resets the DNS client resolver cache.

Incorrect Answers:
B: The new servers are database servers and they are not doing any special services in the domain. It is not necessary to add SRV (service) records for them.
C: Disabling dynamic updates on the DNS Server would prevent Windows 2000 computers from registering themselves in the DNS zone. It would help in registering the two UNIX servers in the zone.
E: The DNS client resolver cache, not the DNS server cache has to be cleared.

QUESTION NO: 27
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The network includes two subnets. Each one has its own domain controller. Subnet1 includes a Windows 2000 server named DNS1, which is configured with a standard primary zone. Subnet2 includes a UNIX server named DNS2, which is configured with a secondary DNS zone. DNS2 successfully accepts zone transfers from DNS1.

All client computers on your network are DHCP clients. The DHCP server is configured to issue the IP addresses of DNS1 and DNS2 to client computers for name resolution.

Users report that they sometimes cannot log on to the domain or perform LDAP searches of the directory. You discover that this problem occurs only when DNS1 is taken offline for maintenance. Users report no other problems accessing resources on the network.

You need to ensure that users can log on to the domain and search the directory even when DNS1 is unavailable. What should you do?

    A.   Configure DNS1 to allow BIND secondary servers
    B.   Configure DNS1 to allow zone transfers to any DNS server
    C.   Install Kerberos v5 client software on DNS2
    D.   Upgrade the DNS server software on DNS2 with a BIND 8.2 compatible implementation

Answer: D
Explanation: In this scenario the users cannot logon or perform LDAP searches when only the UNIX DNS is online. This is because the UNIX DNS server uses an old BIND standard which does not support service records (SRV RRs).To support service records (SRV RRs) and dynamic updates of DNS (DDNS) the Berkeley Internet Name Domain (BIND) 8.2 or later must be used on the UNIX DNS servers. Clients in a Windows 2000 network look up SRV RRs in the DDNS server to locate the network's Active Directory (AD) and its services, in particular the logon service. When a Windows 2000 client system logs on, it queries the DNS server for the domain controllers of the logon domain. Windows 2000 uses SRV RRs to locate the logon service, then sends the client the domain controllers' names. The client uses an available domain controller to log on to the AD domain.

Incorrect Answers:
A: Bind secondaries determines whether to use fast transfer format when transferring a zone to DNS servers running legacy Berkeley Internet Name Domain (BIND) implementations. But the problem at hand is not with zone transfers, it concerns logon and LDAP searches.
B: This is not a zone transfer problem. Users are able to use DNS2 for name resolution when DNS1 is offline. The problem is that they cannot log on to the domain or perform LDAP searches of the directory when DNS1 is offline.
C: Kerberos v5 client is an administrative tool for managing Kerberos security on UNIX systems. It cannot solve the problem at hand. The UNIX DNS server has to be upgraded to BIND 8.2 or later.

QUESTION NO: 28
You are the administrator of TestKing's network, which consists of a single site. The network contains 200 computers running Windows 2000 server and 9,000 computers running Windows 2000 Professional. Every morning, an additional 5,000 manufacturing computers are brought online by using Wake-On-LAN, 15 minutes before the production day begins.

All client computers use DHCP for automatic IP addressing. All servers use static IP addressing. One server runs WINS.
You install a second WINS server on one of your existing domain controllers. You configure DHCP so that one-half of the client computers use the new WINS server as their primary WINS server. The other half use the original WINS server as their automatic primary WINS server. You configure both WINS servers to use the automatic partner configuration.

After the installation, you notice a large number of rejected name registrations in the event log and an increase in network traffic, you also notice a decrease in system performance on the new WINS server.

You want to improve the performance of the new WINS server. What should you do?

    A.   Configure the WINS servers as push partners with each other
    B.   Configure the WINS servers as pull partners with each other
    C.   Change the burst handling setting on the new WINS server to **High**
    D.   Disable burst handling on the new WINS server

Answer: C
Explanation: Windows 2000 WINS servers have the ability to handle high-impact times, like when the 5000 client computers go online every morning as in this scenario, using WINS burst handling. WINS burst handling is disabled by default. When it is enabled it has four settings: Low, Medium (the default setting), High and Custom. WINS burst handling works by handling WINS registration queries by immediately responding positively with a low Time to live (TTL) setting.

Incorrect Answers:
A: This is not a WINS replication problem, it is a WINS registration problem during periods of high impact WINS registration queries.
B: The WINS servers are already configured as pull partners, since this is the default setting.
D: By disabling WINS burst handling WINS performance would suffer during periods of high impact WINS registrations requests.

QUESTION NO: 29
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The network includes 10 Windows 2000 server computers and two NetWare 4.1 servers. The Windows 2000 server computers have static IP addresses and use TCP/IP as their only transport protocol. All client computers run Windows 2000 Professional and use both TCP/IP and IPX/SPX as transport protocols. All client computers are DHCP clients.

You add 50 new client computers to your network. All run Windows 2000 Professional. Many users now report that they experience intermittent connection failures. Connectivity to the NetWare servers remains unaffected, and workgroup resources remain accessible.

You inspect the TCP/IP configuration of a client computer that is currently experiencing a connection failure. You discover that this computer uses the IP address 0.0.0.0

How should you correct the connectivity problem?

    A.   Decrease the lease duration on the DHCP scope to three days

B.   Add a sufficient number of new addresses to the DHCP scope to accommodate the new client computers

C.   Create a new scope on the DHCP server to include the new client computers

D.   Add reservations in the DHCP scope for all client computers

Answer: B

Explanation: The IP address 0.0.0.0 of the client indicates that the DHCP server was not able to give it an IP address. The most likely cause of this is that the DHCP server simply had run out of free IP addresses. 50 clients were added to the network and the DHCP scope must be increased accordingly.

Incorrect Answers:

A: The default lease duration is 8 days. By decreasing the lease duration to 3 days there might be some improvement on IP address availability, since IP addresses are released quickly, but it would not solve the problem in general. Specifically it would not work if the client computers are used concurrently.

C: It is not necessary to create a new scope. The current scope could be extended.

D: Adding reservations for all client computers would not increase the number of available IP addresses.

QUESTION NO: 30

You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The network includes three Windows 2000 domain controllers. All three have the DNS server service installed. Each DNS server hosts an Active Directory integrated zone and requires secure dynamic updates.

The network contains 200 client computers running Windows NT Workstation 4.0. All 200 have static IP addresses and static A (host) records in the DNS zone file.

You upgrade the client computers to Windows 2000 Professional and configure them as DHCP clients. Your DHCP server is configured to always update client records in DNS.

After the upgrade, users report that they cannot access certain workgroup resources on the network. When you examine the DNS zone, you discover that the A records of your client computers are not being updated.

You need to ensure that the DHCP server updates the A records in the DNS zone. You must accomplish this goal with the least possible disruption to client computers.

What should you do?

A.   On the DNS zone file, run DnsCmd.exe with the /AgeAllRecords option

B.   On the DNS zone file, run DnsCmd.exe with the /StartScavenging option

C.   Delete the A records of your client computers from the DNS zone file. Run the ipconfig/registerdns command on the client computers

D.   Delete the A records of your client computers from the DNS zone file. Run the Reconcile Scope command in the DHCP to refresh the records in the DNS zone.

Answer: A
Explanation: Previous versions of Microsoft operating systems that do not support dynamic Domain Name System (DNS) require that a static DNS entry use a static IP address whenever possible. If we upgrade to Microsoft Windows 2000 and our present DNS server is Windows 2000, the IP address will remain the same, but the DNS "A" record remains static. However, the static PTR record is converted to a dynamic entry and is subject to the aging process. The Windows 2000 Dynamic Domain Name System (DDNS) client does not overwrite an existing "A" record if the IP addresses match. To convert static entries to dynamic entries, we must use the /AgeAllRecords option in the Dnscmd.exe command.

Reference: Windows 2000 documentation, Understanding aging and scavenging

Incorrect Answers:
B: The scavenging process removes stale records from the DNS zone. This will not remove the old A (host) records in this scenario sense they are static. These records must first be converted to dynamic entries.
C: Manually deleting all A (host) records for the client computers and then manually configuring every client is a daunting administrative task. It's better to use the /AgeAllRecords option in the Dnscmd.exe program.
D: Deleting all A (host) records for the client computers requires administrative effort. Scope reconciliation of the DHCP database is to add database entries for the existing leases. But there are no existing leases.

QUESTION NO: 31
You are the administrator of TestKing's network. The network consists of 10 Windows 2000 Server computers, 100 Windows 2000 Professional computers, and 150 Windows NT Workstation computers. For workgroup collaboration and document sharing, all client computers have file and print sharing services enabled. You are using DHCP to automate the TCP/IP configuration of all client computers.
You want to accomplish the following goals:

- **All client computers will be able to be located on the network by the network's fully qualified domain name.**
- **A (host) records for all client computers will be automatically added to the DNS zone files.**
- **PTR (pointer) records for reverse name lookup for all client computers will be automatically added to the DNS zone files**
- **A records and PTR records will be automatically removed from the DNS zone files when the DHCP lease expires**

You take the following actions:

- **Configure the DHCP server to always update client computer information in DNS**
- **Configure the DHCP server to discard forward lookups when the lease expires**
- **Configure the DHCP server to update DNS for client computers that do not support dynamic updates**
- **Configure the DHCP scope to configure the domain name for all DHCP client computers.**

Leading the way in IT testing and certification tools, www.testking.com

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

A. All client computers are able to be located on the network by the network's fully qualified domain name.
B. A records for all client computers are automatically added to the DNS zone files.
C. PTR records for reverse name lookup for all client computers are automatically added to the DNS zone files
D. A records and PTR records are automatically removed from the DNS zone files when the DHCP lease expires.

Answer: A, B, C, D
Explanation: If the DHCP server is configured to Always update forward and reverse lookups, it will update both A and PTR resource records itself regardless of the DHCP clients request.
Windows NT machines can be located by their Fully Qualified Domain Name since 'Configure the DHCP server to always update client computer information in DNS' is selected. In Dynamic DNS (DDNS) and DHCP environment like in this scenario, the DHCP Service cleans up both the A records and PTR records in the zone when the lease expires.

QUESTION NO: 32
You are the administrator of TestKing's network. The network is configured as shown in the exhibit.
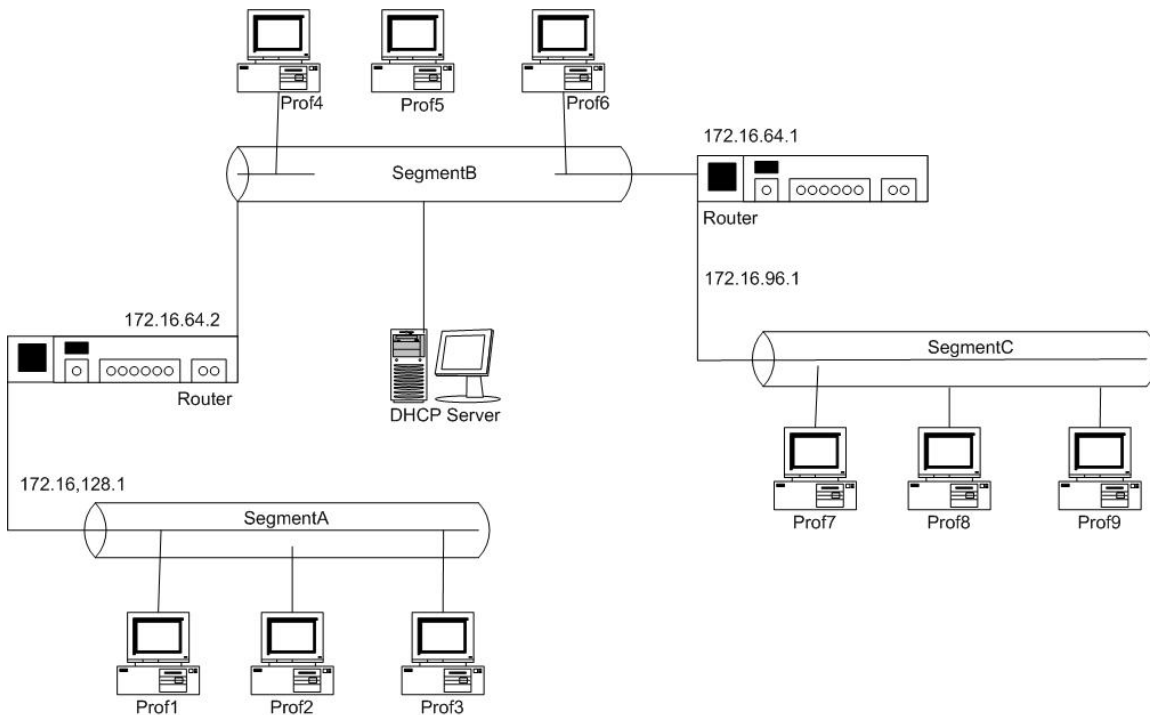
All client computers on your network receive their IP address information from the DHCP server. The user on Prof4 accesses most of his network resources from computers on SegmentA. The users on Prof5 and Prof6 access most of their resources from computers on segment C.

You want to configure your DHCP server to issue gateway addresses Prof4, Prof5 and Prof6. You want these gateway addresses to offer optimum access time.
How should you configure your DHCP server? (Choose Two)

    A.   Create a reservation for Prof4. For this reservation, configure the router option that has the value of 172.16.64.2.
    B.   Create a reservation for Prof5 and Prof6. For each reservation, configure the router option that has the value of 172.16.64.2.
    C.   Configure the DHCP server's **Predefined Router** option so that it has the value of 172.16.64.2.
    D.   Configure the DHCP server **Predefined Router** option so that it has the value of 172.16.64.1.
    E.   On the DHCP server's scope for Segment B, configure the **Router** options so that it has the value of 172.16.64.2.
    F.   On the DHCP server scope for Segment B, configure the **Router** options so that it has the value of 172.16.64.1.

Answer: A, F
Explanation: By configuring the Router option to the value of 172.16.64.1 on the DHCP server's scope for Segment B, the DHCP clients on segment would be configured with this Default Gateway setting, which is the gateway to segment C. By configuring a reservation for the client Prof4 with the router option 172.16.64.2 Prof4 would be the only client on Segment B with a Default Gateway setting of 172.16.64.2, which is the gateway to segment A.

Incorrect Answers:
B: By create a reservation for Prof5 and Prof6 with router option 172.16.64.2 these clients would have a default gateway to Segment A. They mostly use resources on Segment C.
C: There is no Predefined Router Option to be configured at the DHCP Server.
D: There is no Predefined Router Option to be configured at the DHCP Server.
E: The Router option of the DHCP scope on segment B should be configured to 172.16.64.1 not 172.16.64.2. If it is configured with 172.16.64.2 the default gateway would be to segment A not segment B:

QUESTION NO: 33
You are the administrator of TestKing's network. The network consists of 10 Windows 2000 Server computers, 100 Windows 2000 Professional computers, and 150 Windows NT Workstation computers. For workgroup collaboration and document sharing, all client computers have file and print sharing services enabled. You are using DHCP to automate the TCP/IP configuration of all client computers.

You want to accomplish the following goals:

- **All client computers will be able to be located on the network by the network's fully qualified domain name.**
- **A (host) records for all client computers will be automatically added to the DNS zone files.**
- **PTR (pointer) records for reverse name lookup for all client computers will be automatically added to the DNS zone files.**
- **A records and PTR records will be automatically removed from the DNS zone files when the DHCP lease expires**

You take the following actions:

- **Configure the DHCP server to never update client information in DNS**
- **Configure the DHCP server to discard forward lookups when the lease expires**
- **Configure the DHCP scope to configure the domain name for all DHCP client computers**

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

A.   All client computers are able to be located on the network by the network's fully qualified domain name.
B.   A records for all client computers are automatically added to the DNS zone files
C.   PTR records for reverse name lookup for all client computers are automatically added to the DNS zone files
D.   A records and PTR records are automatically removed from the DNS zone files when the DHCP lease expires

Answer: D
Explanation: In Dynamic DNS (DDNS) and DHCP environment like in this scenario, the DHCP Service cleans up both the A records and PTR records in the zone when the lease expires.

Incorrect Answers:
A: Windows NT 4.0 does not support dynamic DNS and Windows NT clients cannot register themselves in DNS. The DHCP server is configured to never update client information in DNS. Therefore A (Host) records and PTR (pointer) will not be added for the Windows NT clients. Furthermore, the Windows NT clients cannot be located by their domain names.
B: The DHCP server is configured to never update client information in DNS. Therefore A (Host) records will not be added for the Windows NT clients.
C: The DHCP server is configured to never update client information in DNS. Therefore PTR (pointer) records will not be added for the Windows NT clients.

QUESTION NO: 34
You are the administrator of TestKing's network. The network consists of five subnets that are connected by a BOOTP relay-enabled router. There are 50 Windows 2000 Server computers and 1,000 Windows

2000 Professional client computers distributed approximately evenly across the five subnets. There are also 25 UNIX servers and 100 DHCP-enabled network printers on the network.

You want to accomplish the following goals:

- **The correct assignment of IP addresses to each client computer on each subnet will be automated.**
- **Address conflicts between client computers and servers will be prevented**
- **Correct scope options will be applied to each client computer on each subnet.**
- **Client computers that are not in use will be prevented from keeping an IP address for more than three days.**
- **Each network printer will always receive the same IP address**

You take the following actions:

- **Install the DHCP Server service on a Windows 2000 Server computer.**
- **Create five scopes, each containing the address range for a specific subnet**
- **In the DHCP console, set optional client configurations for each scope in the Scope Options container**
- **Exclude the range of addresses in use by the servers**
- **Exclude the range of addresses in use by the network printers.**

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

A.   The correct assignment of IP addresses to each client computer on each subnet is automated
B.   Address conflicts between client computers and servers are prevented.
C.   Correct scope options are applied to each client computer on each subnet.
D.   Client computers that are not in use are prevented from keeping an IP address for more than three days.
E.   Each network printer always receives the same IP address

Answer: A, B, C
Explanation: The DHCP Server service is installed. Five scopes have been created, each containing the address range for a specific subnet'. This ensures an automated assignment of IP addresses and scope options to every client computer on the five subnets.
By excluding the range of addresses used by the servers no address conflicts between client computers and servers will occur.

Incorrect Answers:
D: The DHCP lease duration has not been configured. Furthermore, the default DHCP lease duration is 8 days, not 3 days.
E: The printers have been excluded from the Scope range. This will not, by itself, configure the IP address for the printers. Reservations for the printers should be added.

QUESTION NO: 35
You are the administrator of a Windows 2000 network. The network consists of two Windows 2000 Server computers named Atlanta and Orlando and 350 Windows 2000 Professional computers.

Orlando is a DHCP Server. The DHCP Server provides the TCP/IP configuration of all the Windows 2000 Professional computers. Atlanta and Orlando have IP Addresses that are manually configured. Atlanta frequently hosts multicast-based video and audio conferences. You want to dynamically allocate multicast addresses.

How should you configure the network?

A.   On the DHCP Server, create and activate a scope that it has range of Class D addresses.
B.   On Atlanta, configure Routing and Remote Access to enable the IGMP routing protocol in Proxy mode on the LAN interface.
C.   On the Windows 2000 Professional computers, enable router discovery.
D.   On the Windows 2000 Professional computers, add a route for network destination 224.0.0.0 and mask 224.0.0.0.

Answer: A
Explanation: To dynamically allocate multicast addresses we require a DHCP server with a scope for the multicast addresses. The class D addresses range from 224.0.0.0 to 239.255.255.255. These addresses are used for multicasting, in which datagrams flow to a group of recipients instead of to a single recipient (unicasting). Multicasting has applications in streaming audio and video transmission.

Incorrect Answers:
B: The IGMP routing protocol in Proxy mode is only used when there is router not supporting multicast routing. In this scenario the two routers communicate directly with each other and there are no routers in between.
C: Windows 2000 supports router discovery as a host and router. This is not configured at clients. To dynamically allocate multicast addresses the DHCP server is used.
D: To dynamically allocate multicast IP addresses you configure a scope at the DHCP server, not by configuring a route on the client computers.

QUESTION NO: 36
You are the administrator of TestKing's network. The network consists of one Windows 2000 domain that has 10 Windows 2000 Server computers and 500 Windows 2000 Professional client computers.

You want all client computers to receive their TCP/IP configuration from DHCP. You install the DHCP Server service on one of your Windows 2000 Server computers and create and activate a scope of addresses.

Leading the way in IT testing and certification tools, www.testking.com

Users report that they cannot connect to the network. You discover that none of the client computers are receiving TCP/IP configurations from DHCP.
What should you do to resolve this problem?

    A.   Stop and restart the DHCP Server service on the DHCP server
    B.   Restart all client computers
    C.   Authorize the DHCP server in Active Directory
    D.   Add a DNS host record for the DHCP server

Answer: C
Explanation: Before DHCP servers are allowed to run in a Windows 2000 domain they need to be authorized in the Active Directory of the domain. This is done by opening the DHCP Server Console, right-click DHCP, select Manage authorized servers, select Authorize, and type name or IP address of the DHCP server to be authorized.

Incorrect Answers:
A: The DHCP Server service cannot be started until it is authorized in the Active Directory.
B: No user can connect to the network, so restarting the clients will not help. The DHCP Server must be authorized.
D: The client computers broadcast to initiate communication with the DHCP server. Then they are able to communicate by the IP address of the DHCP server. The name of the DHCP server is not needed.

QUESTION NO: 37
You are the enterprise administrator of a Windows 2000 domain. The domain has three Windows 2000 Server computers named Athens, Barcelona and Cairo, and 90 Windows 2000 Professional computers.

Your network consists of three segments connected by a router. Each segment contains one of the servers. The 90 Windows 2000 Professional computers are evenly distributed over the three subnets pic says segments.

Athens is a DHCP server. The TCP/IP configuration of all the Windows 2000 Professional computers on the three segments is provided by the Athens DHCP server. The DHCP server has three scopes, one for each segment. The lease time for all these scopes is eight days.

For performance reasons you want to move the DHCP server service from Athens to Barcelona.

You take the following actions:

- **On Athens, stop and disable the DHCP server service.**
- **On Barcelona, install, authorize, and stop the DHCP server service.**
- **Copy the entire *system root\system32\dhcp* folder from Athens to Barcelona.**

You want to configure Barcelona to use the scope information and the leased addresses currently in use by the Windows 2000 Professional computers.

What should you do next on Barcelona? (Choose Two)

A. Enable DHCP Relay Agent. Use a boot threshold of 0 seconds.
B. Use the Jetpack utility to manually repair the DHCP database.
C. Use the Regedt32.exe registry editor to restore the DHCP registry configuration from the *systemroot\system32\Dhcp\backup* location.
D. Copy the *system root*\system32\DHCP\j50.chk file to the Dhcp.mdb file.
E. Start the DHCP server and reconcile all scopes.
F. Start the DHCP server and create a new superscope that contains the three original scope ranges.

Answer: C, E
Explanation: To move the DHCP Database we must first stop the DHCP service on the old server, back up the Registry key HKLM\SOFTWARE\Microsoft\DhcpServer\Configuration, and install DCHP on the new server. We must then stop the DHCP service on the new server and restore the Registry key from the old server onto the new server. Then we must delete the contents of C:\WINNT\System32\DHCP on the new server, copy the database file DHCP.MDB from the old server onto the new server but not the transaction logging (*.LOG) and checkpoint (*.CHK) files and start the DHCP Service on the new server. Finally we must reconcile all scopes on the new server to synchronize the database with the Registry.

Incorrect Answers:
A: A DHCP relay agent is not needed to install and configure the new DHCP Server.
B: It is not necessary to repair the DHCP database when it is moved.
D: The DHCP.MDB file should simply be copied from the old to the new server. Copying the *system root*\system32\DHCP\j50.chk file to the Dhcp.mdb file is incorrect.
F: It is not necessary to create a superscope, instead all scopes should be reconciled on the new server.

QUESTION NO: 38
You are configuring a Windows 2000 Professional computer as a client computer in TestKing's network. The servers in the network consist of a mix of Windows 2000 Server computers, Windows NT 4.0 computers, and NetWare 3.11 and 4.1 servers.

You install and configure both TCP/IP and NWLink IPX/SPX on the Windows 2000 Professional computer. You also install the client software for both Microsoft and NetWare networks. When you attach the computer to the network, you can communicate with all of the Windows-based servers and the NetWare 4.1 servers, but you cannot see the NetWare 3.11 servers in My Network Places. You also cannot map drives by using either Microsoft-specific or NetWare-specific commands.

What should you do to correct this problem?

A.   Edit the NetworkNumber value in the registry to specify the network number for the NetWare 3.11
      servers.
B.   Edit the NetworkNumber value in the registry to specify the network number for the NetWare 4.1
      servers.
C.   Edit the NetworkNumber value in the registry to specify the network number for both the NetWare
      3.11 and 4.1 servers.
D.   Edit the PktType value in the registry to include the hexadecimal value for the 802.2 frame type.
E.   Edit the PktType value in the registry to include the hexadecimal value for the 802.3 frame type.
F.   Edit the PktType value in the registry to include the hexadecimal value for both the 802.2 and 802.3
      frame types.

Answer: F
Explanation: NetWare 3.11 uses the 802.3 frame type. Netware 3.12 and above uses the 802.2 frame type. This
network has both NetWare 3.11 and NetWare 4.1 servers, so both Frame Types must be installed. Installation of
multiple frame types on a Windows 2000 Professional requires editing of the Registry, specifically add both
types to the multi-string value PktType in
HKLM\SYSTEM\CurrentControlSet\Services\NwlnkIPX\Parameters\Adapters\<ID>, where <ID> is the
network adapter identifier.

Incorrect Answers:
A: Network numbers values denote a network segment. There is no specific network segment for NetWare
         3.11 servers.
B: Network numbers values denote a network segment. There is no specific network segment for NetWare
         4.1 servers.
C: Network numbers values denote a network segment. There is no specific network segment for NetWare
         3.11 or NetWare 4.1 servers.
D: The 802.3 frame type must be added as well since there are Netware 3.11 servers on the network.
E: The 802.2 frame type must be added as well since there are Netware 4.1 servers on the network.

QUESTION NO: 39
**You are the administrator of TestKing's network. Your Web server is configured to run a third-party
Web application for users on your network.**

**Another network administrator in your company has recently made some configuration changes to
secure the server. Users report that each time they try to connect to a secure Web page stored on the Web
server, they receive the following error message, "Web page requested is not available". Users have no
problem connecting to FTP, and you have verified that the web service has started.**

**You want to discover why users are receiving the error message. What should you do to diagnose the
problem?**

A.   Verify that port 21 and port 20 are permitted in your TCP/IP filter.

B.   Verify that port 443 is permitted in your TCP/IP filter.
C.   Verify that the connect NTFS file permissions are on the Web pages.
D.   Verify that the port 80 is permitted in your TCP/IP filter.

Answer: B
Explanation: Port 443 is used for secure web traffic (HTTPS). Therefore TCP/IP should permit this port.

Incorrect Answers:
A: Port 20 and port 21 are used for FTP traffic.
C: This is not a permission problem, the web page that was requested was not available.
D: Port 80 is the HTTP protocol. HTTPS, secure web server, is port 443.

QUESTION NO: 40
You are the administrator of a Windows 2000 network. You need to assign network ID numbers and host addresses to the computers in one of TestKing's branch offices.

A single route to the branch office is advertised as 192.168.16.0/21. The branch office has 150 computers on a single subnet of 192.168.16.0/24. However, the company wants to be able to add up to another 2,000 computers to the branch office.

You want to be able to accommodate all computers in the branch office, while also taking advantage of route summarization. Which steps should you take to achieve this goal? (Choose all that apply)

A.   In the branch office, add another route advertised as 192.168.32.0/22.
B.   In the branch office, add additional network numbers ID numbers 192.168.33.0/24 – 192.168.39.0/24.
C.   In the branch office, add additional network ID numbers 192.168.17.0/24 – 192.168.23.0/24.
D.   In the branch office, add additional network ID numbers 192.168.24.0/24 – 192.168.31.0/24.
E.   Change the advertisement to the branch office to 192.168.16.0/20

Answer: D, E
Explanation: In this scenario there are 150 computers at the branch office now, but up to 2000 computers could be added in the future. To accommodate for all clients 12 bits will be needed for the clients (2**12=4096). A network mask of 20 bits (32 minus the 12 hosts bits) or less is acceptable. The 192.168.16.0/20 TCP/IP configuration could be used. This range could be used to add 8 additional network ID numbers 192.168.24.0/24 - 192.168.31.0/24. This range is subnetted within 192.168.16.0/20 - or 192.168.16.0/20 is a supernet of the 192.168.24.0/24 - 192.168.31.0/24 networks. This would supply more than 2000 hosts: 8 networks with 254 hosts each equals 2032 hosts.

Note: The networks are
192.168.24.0/24 (first)

192.168.25.0/24 (we add 1 in the network partition - that is we add 0.0.1.0)
192.168.26.0/24
192.168.27.0/24
192.168.28.0/24
192.168.29.0/24
192.168.30.0/24
192.168.31.0/24 (last)

Incorrect Answers:
A: With a 22 bit subnet mask (192.168.32.0/22) only 1022 (2**10-2) hosts could be used. Here we need to supply more than 2000 hosts.
B: The 192.168.33.0/24 – 192.168.39.0/24 range is not contiguous and it supplies only 7 network IDs with 254 hosts each which is less than the required 2000 hosts.
C: 192.168.17.0/24 – 192.168.23.0/24 only gives 7 new network ID numbers. Each network has 254 hosts (2**(32-24)-2 hosts). 7 network IDs would only supply 1774 clients. 8 Network ID numbers are needed.

QUESTION NO: 41
You are the administrator of TestKing's network. Your network is configured as shown in the exhibit.
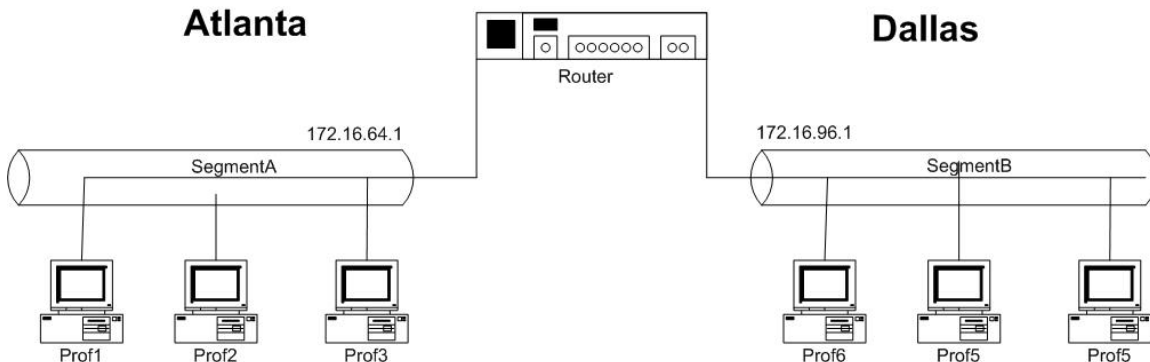
You investigate a report that administrators in the Dallas office have installed and are using Network Monitor. Your company allows only administrators in the Atlanta office to install and use Network Monitor.

You install Network Monitor on Prof1. You need to monitor how many copies of Network Monitor are currently running.

What should you do? (Choose Two)

A.   On the **Tools** menu in Network Monitor, select **Identify Network Monitor Users.**
B.   On the **Options** menu in Network Monitor, select **Show Address Names.**

C.   On the **Tools** menu in Network Monitor, select **Find Routers**.
D.   On the **Display** menu in Network Monitor, select **Find all names.**
E.   Install Network Monitor on a computer on SegmentB.
F.   Permit all ports in the TCP/IP filter on the router.

Answer: A, E
Explanation: In Network Monitor, the "Identify Network Monitor users" option is available in the Tools menu. This option sends a series of multicast packets to all NetBIOS- enabled systems that have the Network Monitor agent installed. After detecting all the Network Monitor agents, a list of the agents is displayed. It will show other computer's names that are running network monitor along with the user name, MAC address, network monitor state (running, capturing, or transmitting), and network monitor version.
In order to detect installations of Network Monitor on segment B the Network monitor has to be installed on a computer on SegmentB.

Incorrect Answers:
B: The Show Address Names command in the Options menu toggles whether or not friendly names are used. It is enabled by default. It is not required to monitor how many copies of Network Monitor are currently running.
C: The Find Routers command finds routers, it does not find computer running Network monitor.
D: There is no Display menu in Network Monitor.
F: It is not necessary to permit all ports in the TCP/IP filter on the router.

QUESTION NO: 42
You are the administrator of a Windows 2000 network that has a main office and one branch office. You use PPTP to connect the main office to the branch office.

You want to verify that the strongest possible level of data encryption is supported for the connection.

What should you do?

A.   In the Routing and Remote access consoles, verify that the dial-in profile used to establish the connection between the two offices allows only MS-CHAP.
B.   In the properties of the Routing and Remote Access Server objects in the Routing and Remote access consoles, verify that the Extensible Authentication Protocol is using MD5-CHAP.
C.   In the properties of the PPTP interfaces in the Routing and Remote Access consoles, verify that MS-CHAP v2 is being used as the authentication method.
D.   In the properties of the PPTP interfaces in the Routing and Remote Access consoles, verify that Password Authentication Protocol (PAP) is being used as the authentication method.

Answer: B

Explanation: We can use EAP to support authentication schemes such as Generic Token Card, MD5-Challenge (MD5-CHAP), Transport Level Security (TLS) for smart card support, and S/Key as well as any future authentication technologies. Extensible Authentication Protocol using MD5-CHAP is more secure than MS-CHAP V2, MS-CHAP and PAP.

Note: The Message Digest 5 Challenge Handshake Authentication Protocol. This protocol encrypts user names and passwords with an MD5 algorithm.

Incorrect Answers:
A: CHAP uses encrypted authentication but is vulnerable.
C: MS-CHAP V2 is an improvement on CHAP. In MS-CHAP the challenge response is calculated with a Message Digest 4 (MD4)-hashed version of the password
D: PAP uses plaintext and is not a secure authentication protocol.

QUESTION NO: 43
You are the administrator of your company. To monitor the traffic on your network, you install Network Monitor. You need to monitor the source IP address, and destination IP address, and destination port number of every TCP/IP frame on the network. You want to log this information for a period of three hours.

What should you do? (Choose Two)

   A.   On the **Capture Buffer Settings** menu, increase the buffer size.
   B.   On the **Capture Buffer Settings** menu, decrease the buffer size.
   C.   On the **Capture Buffer Settings** menu, increase the frame size.
   D.   On the **Capture Buffer Settings** menu, decrease the frame size.
   E.   Change the Temporary Capture Directory.

Answer: A, D
Explanation: In this scenario the buffer size must be increased from the default setting of 1.0 MB to prevent to buffer from being overwritten. By decreasing the frame size from the default value of 65,535 bytes, the buffer will last longer before it is overwritten.

Incorrect Answers:
B: In this scenario the buffer size must be increased not decreased.
C: The frame size must be decreased not increased.
E: To only reason for moving the Temporary Capture Directory is that the hard drive is becoming full. It is no indication in this scenario that this is the case.

QUESTION NO: 44
You are the administrator of a mixed Windows NT 4.0 and Windows 2000 network. All of the Windows 2000 Server computers in your network are member servers of a single Windows NT 4.0 domain. You want to use two of these servers to test configurations of IPSec that are using the Kerberos authentication protocol.
What should you do?

    A.   On both servers, create a new IPSec policy.
            Configure a rule so that it will not use a tunnel.
            Specify shared secret key authentication.
            Assign the new policy.
    B.   On one of your servers, install a stand-alone root Certificate Authority (CA).
            Create a digital certificate for both servers.
            On both servers create a new IPSec policy and specify the issued certificate for authentication.
            Assign the policy.
    C.   On both servers, create a new IPSec policy.
            Specify the tunnel end point as the IP address of the partner Server and specify a shared secret key to use for authentication.
            Assign a new policy.
    D.   Promote one of the servers to a domain controller.
            Assign the domain controller as the default Secure Server IPSec policy.
            Assign the other Server the default Client IPSec policy.

Answer: D
Explanation: Active Directory is needed for Kerberos Authentication. Kerberos is not supported in Windows NT 4.0. Therefore we must promote one of the Windows 2000 member servers to a domain controller, use Secure Server (Require encryption) on this domain controller and configure the other server with the Client IPSec Policy. To promote a Windows 2000 member server to a domain controller we must install Windows NT 4.0 as a backup domain controller (BDC), promote the BDC to a primary domain controller (PDC), and then promote to Windows 2000 mixed-mode domain controller.

Incorrect Answers:
A: A Windows 2000 domain controller is required for Kerberos authentication.
B: A Windows 2000 domain controller is required for Kerberos authentication.
C: A Windows 2000 domain controller is required for Kerberos authentication.

QUESTION NO: 45
You are the administrator of TestKing's network. Network is configured as shown in the exhibit.
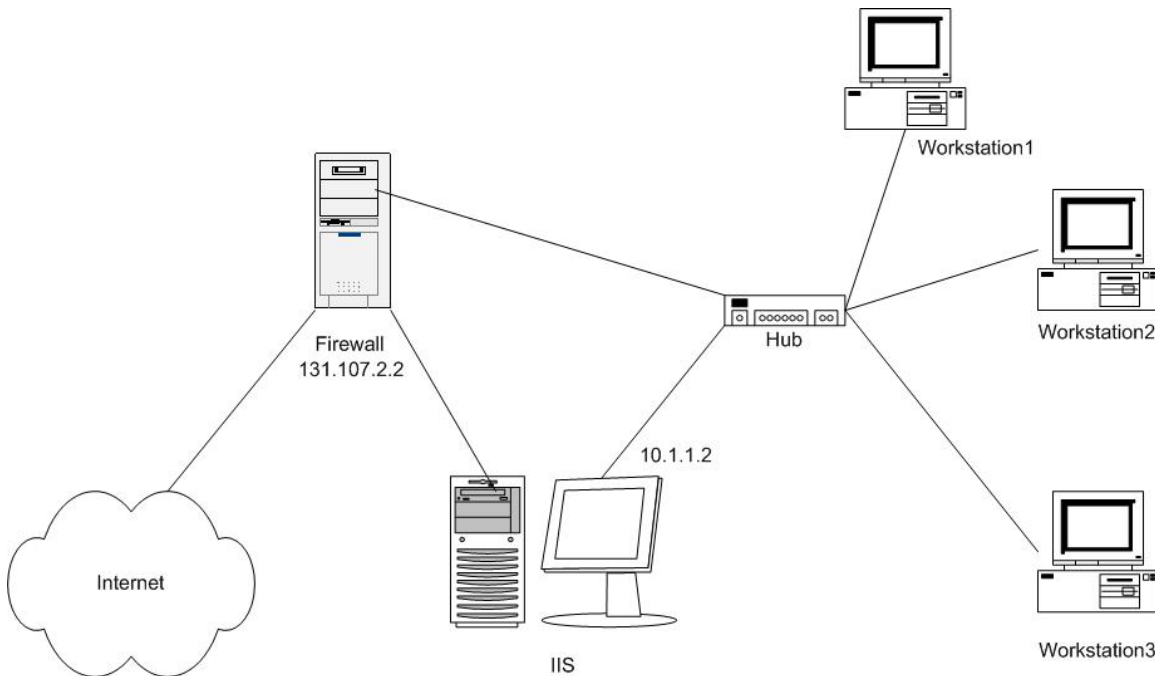
You are configuring your Windows 2000 server computer that runs Internet Information Server (IIS). Your Server uses the IP address of 131.107.2.2 to support Internet users. Your server uses the IP address of 10.1.1.2 to support an intranet application.

You want to configure your server to permit only Web communications from the Internet. You also want to configure your server to allow access to shared folders and other resources for users on the intranet. What should you do? (Choose two)

A.   Enable a TCP/IP filter. Permit only port 80 on the network adapter that uses the IP address of 131.107.2.2.
B.   Enable a TCP/IP filter. Permit only port 21 and port 20 on the network adapter that uses the IP address of 131.107.2.2.
C.   Permit all ports on the network adapter that uses the IP address of 131.107.2.2.
D.   Enable a TCP/IP filter. Permit only port 80 on the network adapter that uses the IP address of 10.1.1.2.
E.   Enable a TCP/IP filter. Permit only port 21 and port 20 on the network adapter that uses the IP address of 10.1.1.2.
F.   Permit all ports on the network adapter that uses the IP address of 10.1.1.2.

Answer: A, F
Explanation: In this scenario External Internet users will use the 131.107.2.2 IP address to use the Web server. Therefore it should only be enabled for web traffic (HTTP), which uses the TCP port 80. Internal users will use the 10.1.1.2 IP address to access the Web server. Furthermore, all traffic should be permitted.

Incorrect Answers:

B: Port 20 and port 21 which are used for FTP traffic, port 80 is used for http traffic. We should therefore permit port 80 on Internet interface of the Web server.
C: Only port 80 should be permitted on the Internet interface of the Web server.
D: All ports should be permitted on the internal interface of the Web server, not only web traffic.
E: All ports should be permitted on the internal interface of the Web server, not only FTP traffic.

QUESTION NO: 46
You are the administrator of TestKing's network. Your network is configured in a Windows 2000 domain as shown in the following diagram.
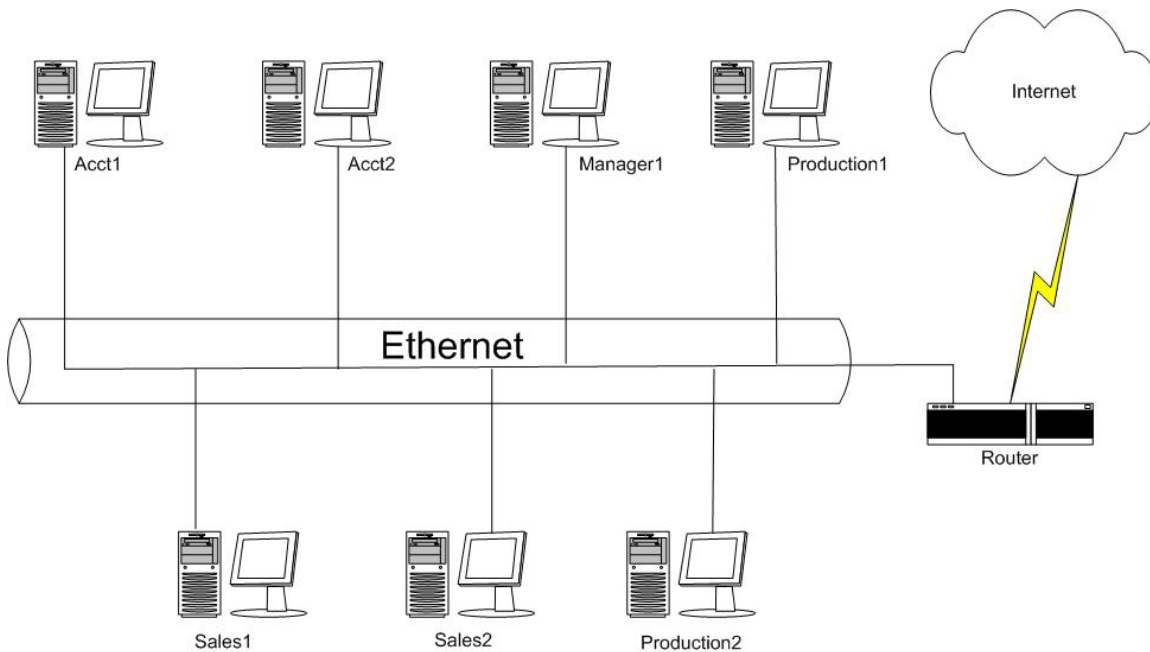
Acct1 and Acct2 belong to the accounting department. Sales1 and Sales2 belong to the sales department. Production1 and Production2 belong to the production department. Manager1 belongs to the management department. The accounting department does not access the Internet.

You want to accomplish the following goals:

- **All communications involving the Acct1 and Acct2 will be encrypted.**
- **Internet communications will not be encrypted.**
- **Communications between the sales department and the management department will be encrypted.**
- **Performance overhead for encryption will be minimized.**

You take the following actions:

▪ **Create an organizational unit (OU) structure as shown in the exhibit.**
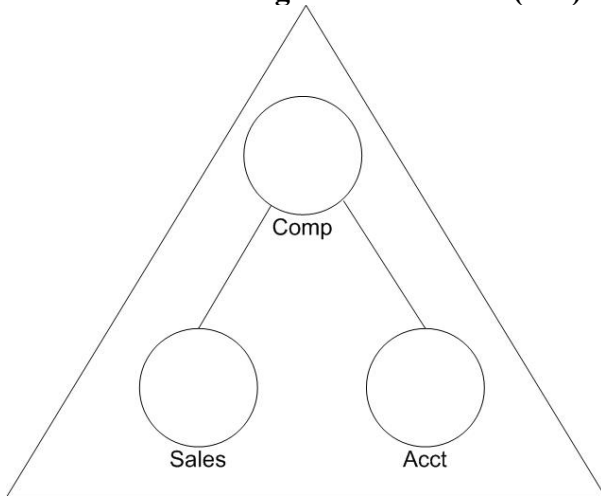
- **Add Acct1 and Acct2 to the ACCT OU.**
- **Add Sales1 and Sales2 to the Sales OU.**
- **Add all other computers to the Comp OU.**
- **Assign the default Secure Server IPSec Policy to the domain.**

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

A. All communications involving Acct1 and Acct2 are encrypted.
B. Internet communications are not encrypted.
C. Communications between the sales department and the management department are encrypted.
D. Performance overhead for encryption is minimized.

Answer: A, C

Explanation: By choosing the Secure Server (Require security) as a default for the Domain all communication would be encrypted; especially all communication involving Acct1 and Acct2, communications between the sales and the managements department, and Internet communication.

Incorrect Answers:

B: By choosing the Secure Server (Require security) as a default for the Domain, all communication with the servers, even Internet communication, would be encrypted.
D: Since even Internet communication is encrypted, even though is not required, the performance overhead for encryption is not minimized.

QUESTION NO: 47
You are the administrator of TestKing's network. The network consists of 10 Windows 2000 Server computers, 200 Windows 2000 Professional computers, 250 Windows 98 computers, and 25 UNIX

workstation computers running SMB server software. The network runs only TCP/IP as its transport protocol. You implement WINS in the network for NetBIOS name resolution.

Users of the Windows-based client computers report that they cannot access resources based on the UNIX computers by NetBIOS name. There is no problem accessing Windows-based resources by NetBIOS name.

What should you do to resolve this problem?

    A.   Install a WINS proxy agent on one of the UNIX computers.
    B.   Install a WINS proxy agent on one of the Windows-based computers.
    C.   On the WINS server, create static mappings for the UNIX computer.
    D.   On the WINS server, create static mappings for the Windows-based computers.

Answer: C
Explanation: In this scenario Windows computers cannot access resources on the UNIX computers. This is because UNIX computers do not register themselves in WINS thus There are no records for the UNIX computers in the WINS server. We can overcome this problem by adding static mappings of the UNIX computers in the WINS server.

Incorrect Answers:
A: The WINS Proxy agent is used to enable non-WINS clients want to communicate with WINS-clients. But in this scenario the non-WINS clients, the UNIX computers, are able to connect to resources on the Windows computers already, Static entries of the UNIX computers have to be added.
B: The WINS Proxy agent is used to enable non-WINS clients want to communicate with WINS-clients. But in this scenario the non-WINS clients, the UNIX computers, are able to connect to resources on the Windows computers already, Static entries of the UNIX computers have to be added.
D: Resources on the Windows computers can already be used. Windows computers have already registered themselves in WINS.

QUESTION NO: 48
You are the administrator of TestKing's network. The network consists of a single Windows 2000 domain. The network has Windows 2000 Server computers, Windows 2000 Professional computers, and Windows NT Workstation 4.0 computers distributed across two IP subnets as shown in the exhibit.
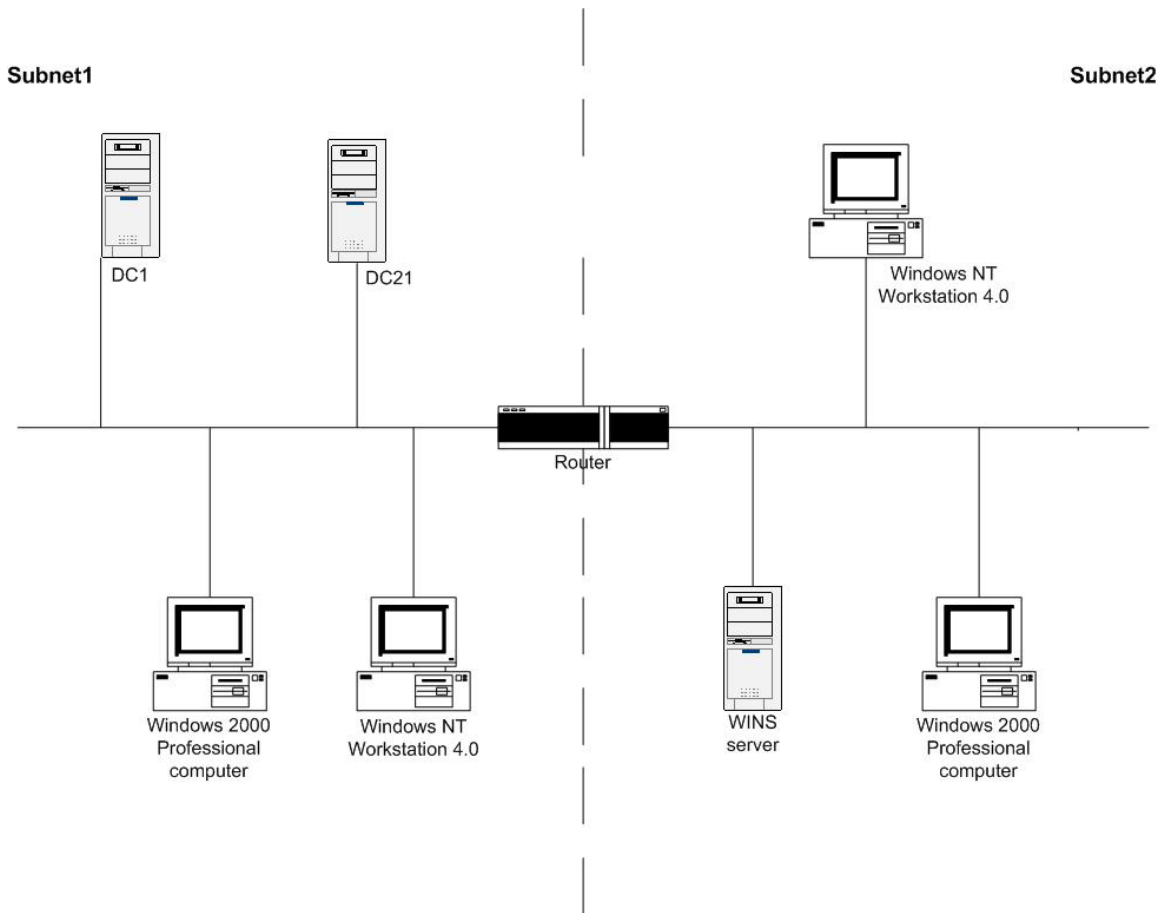
Two Windows 2000 domain controllers are located on Subnet1. Each domain controller is also a DNS server hosting an Active Directory integrated zone. You implement WINS for NetBIOS name resolution on your network. WINS is installed on a server on Subnet2.

Users of the Windows NT Workstation 4.0 computers on Subnet2 report that they are receiving the following error message, "Domain Controller cannot be located". Subsequently, these users cannot be validated on the network. Windows NT Workstation 4.0 users on Subnet1 are not experiencing this problem. However, they do report that response times for logon requests are extremely slow. None of the Windows 2000 Professional users on either subnet report these problems.

You want to ensure that Windows NT Workstation 4.0 users on Subnet2 can be validated. You also want to improve logon request response time for users on Subnet1.

What should you do?

    A.   Configure the router to forward NetBIOS broadcast packets
    B.   Configure the Windows NT Workstation 4.0 computers as DNS clients in the existing zone
    C.   Configure the Windows NT Workstation 4. 0 computers as WINS clients
    D.   Configure the Windows 2000 Server domain controller computers as WINS clients

Answer: D
Explanation: The Windows 2000 computers use DNS for name resolution. Windows 2000 computers do not register themselves in WINS; specifically the Windows 2000 Domain controllers are not registered in WINS. The NT 4.0 clients use WINS for name resolution but they will be unable to find the Domain Controllers by using WINS. The Windows 2000 domain controllers need to be registered in WINS. That is they have to be configured as WINS clients.

Incorrect Answers:
A: The WINS server is on the same segment as the NT 4.0 machines. The NT 4.0 clients will be able to communicate with the WINS server. The Windows 2000 computers on the other segment do not use WINS.
B: The Domain Controllers, not the NT Workstations, must be configured as WINS clients.
C: The Domain Controllers, not the NT Workstations, must be configured as WINS clients.

QUESTION NO: 49
You are the administrator of TestKing's network. The network consists of Windows 2000 Server computers, Windows NT Workstation client computers, and Windows for Workgroups 3.11 client computers distributed across three subnets. All client computers are configured as DHCP client computers to automate TCP/IP configuration.

You install a WINS server on one subnet on your network. You also define a DHCP scope option to include the WINS server's address.

Users report that they can access resources on servers on their own subnet, but they cannot access resources on other subnets.

What should you do to resolve this problem?

- A. Use the **ipconfig/renew** command to refresh the client computers' configuration
- B. Use the **ipconfig/release** command to refresh the client computers' configuration.
- C. Install a WINS proxy agent on the subnet that hosts the WINS server.
- D. Install a WINS proxy agent on the subnets that do not host the WINS server.

Answer: A
Explanation: In this scenario the IP configuration has been updated on the DHCP server. This new information must reach the client computers. To accomplish this we should use the IPConfig /renew command on every DHCP client computer. Windows 3.11 client computers are also able to use the ipconfig/renew command.

Incorrect Answers:
B: Ipconfig/renew not ipconfig/release is used to get new TCP/IP configuration information from the DHCP Server. Ipconfig/release only resets the client's IP configuration.
C: All clients in the network are able to use WINS, therefore it is not necessary for any WINS Proxy agent.
D: All clients in the network are able to use WINS, therefore it is not necessary for any WINS Proxy agent.

QUESTION NO: 50
You are the administrator of a Windows 2000 network. The network has three segments connected by a router. Each segment contains a Windows 2000-based WINS server and two other Windows 2000 Server computers. The network also has 300 Windows NT Workstation 4. 0 WINS client computers distributed evenly over the three segments.

Users in each network segment inform you that they cannot browse any network resources on the other network segments. They do not have problems browsing their own segment.

How should you configure the network to enable users to browse for network resources on all three-network segments?

  A.   Configure all WINS client computers to be NetBIOS node type Mixed (m-node)
  B.   Configure all WINS client computers to use all three WINS servers.
  C.   On each WINS server, configure the Lmhosts file to contain entries that include #PRE and #DOM For the other two WINS servers
  D.   Configure the three WINS servers as replication partners of one another.

Answer: D
Explanation: In this scenario the WINS servers are working in isolation on each segment with no replication of information. They need to exchange their records by setting them up as replication partners. The NetBIOS broadcasts will not pass the routers, but the WINS replication will.

Incorrect Answers:
A: WINS client are h-node (hybrid) by default, that is, they use WINS followed by broadcast. Changing to m-mode (mixed), which is broadcast followed by WINS, will not help since the routers do not pass broadcasts and the WINS servers do not replicate information.
B: The routers will not allow the WINS traffic through.
C: The lmhosts file must be copied to every WINS client computer, not only to the WINS Server computer.

QUESTION NO: 51

You are the administrator of a Windows 2000 network. The network has four Windows 2000-based WINS servers named NY1, NY2, Bos1 and Bos2. The network has computers in two locations: Boston and New York.

The Bos1 and Bos2 Wins servers are at Boston location. The NY1 and NY2 WINS servers are at the New York location.

You want to configure the replication between the WINS servers to accomplish the following goals:

- **The NY1 and NY2 WINS servers must replicate changes in the local database to each other immediately following each new registration or IP address change registration.**
- **The Bos1 and Bos2 WINS servers must replicate changes in the local database to each other every 30 minutes.**
- **The changes in the WINS database in either location should be replicated to the other location every three hours.**

How should you configure the WINS servers to accomplish these goals? (Choose Three)

A. Configure the WINS servers to enable burst handling. Set the number of requests for burst handling to **1.**

B. Configure the NY1 and NY2 WINS servers as push/pull partners of each other. Configure both WINS servers to use persistent connections for push replication partners. Set the number of changes before replication to **1.**

C. Configure Bos1 and Bos2 WINS servers as push/pull partners of each other. Specify a replication interval of 30 minutes.

D. Configure Bos1 and Bos2 WINS servers as push/pull partners of each other. Configure both WINS servers to enable periodic database consistency checking every 30 minutes.

E. Configure the NY1 and Bos1 WINS servers as push partners of each other. Configure both WINS servers to update statistics every three hours.

F. Configure the NY1 and Bos1 WINS servers as push/pull partners of each other. Specify a replication interval of three hours.

Answer: B, C, F
Explanation: By configuring NY1 and NY2 WINS servers as push/pull partners, using persistent connections and setting the number of changes to replication to 1, the WINS servers will be able to replicate any changes to each other immediately. The default setting requires at least 20 changes before replication. Bos1 and Bos2 are configured as push/pull partner with a replication interval of 30 minutes, which forces them to replicate their local databases to each other every 30 minutes. NY1 and Bos1 are configured as push/pull partner with a replication interval of 3 hours, which forces them to replicate their local databases to each other every 3 hours.

Incorrect Answers:
A: Burst handling is only useful for high impact WINS registration periods, and it is not used for WINS replication configuration.

D: The replication interval, not periodic database consistency checking, should be configured to 30 minutes.

E: There is no requirement to update statistics of the WINS servers.

QUESTION NO: 52

You are the administrator of a Windows 2000 network. The network has 18,000 Windows 2000 Professional WINS client computers and six Windows 2000-based WINS servers. The WINS client computers are portable client computers, and they frequently connect to the network at different locations. The WINS client computers access NetBIOS-based resources. The TCP/IP configuration of the WINS client computers is provided by DHCP servers on the network.

Some of the WAN links in your network are unreliable. You want to ensure that all Windows 2000 Professional computers are able to resolve NetBIOS names, even if some of the WINS servers are not available.

How should you configure the network to accomplish this goal?

    A.   On each segment, configure a computer as a WINS proxy.
    B.   Configure the DHCP servers to provide each client computer with a list of WINS servers.
    C.   Configure the WINS servers to enable burst handling. Set the number of requests for burst handling to **High.**
    D.   Configure the DHCP server to set the NetBIOS over TCP/IP node type for each client computer to **Mixed (m-node).**

Answer: B

Explanation: Windows 2000 clients can be configured to use up to 12 WINS Servers. This redundancy would be beneficial in a large network as it will ensure that all Windows 2000 Professional computers are able to resolve NetBIOS names, even if some of the WINS servers are not available.

Incorrect Answers:

A: Since all clients are Windows 2000 computers which are WINS-enabled, a WINS-Proxy is not required.

C: Burst handling could improve performance during high impact WINS registration periods, but it is not used to configure redundancy in case of WINS server failure.

D: Mixed mode, instead of the default Hybrid mode, only switches the order of the WINS communications methods. In hybrid mode WINS is followed by the broadcast and in mixed mode the broadcast is followed by WINS. Therefore mixed mode would not offer any redundancy.

QUESTION NO: 53

You are the administrator of a Windows 2000 network. The network has seven Windows 2000-based WINS servers, and each is in a separate location.

Because network users frequently logon at different locations, you want to configure the seven WINS servers to have a convergence time of less than one hour.

How should you configure the seven WINS servers to accomplish this goal?

A.   Create a display of the seven WINS servers in a circular arrangement.
        Configure each WINS server as a push/pull partner with the two WINS servers beside it in the circle.
        Use a replication interval of 25 minutes.
B.   Designate one of the WINS servers as the central WINS server.
        Configure the other six WINS servers as push/pull partners with the central WINS server. Configure the central WINS server as the push/pull partner with the other six WINS servers.
        Use a replication interval of 25 minutes.
C.   Configure each WINS server to automatically configure the other WINS servers as its replication partners.
        Use the default interval time for automatic partner configuration.
D.   Configure each WINS server to use a renew interval of 50 minutes.
        Use the default value for verification interval.

Answer: B
Explanation: The Default WINS Pull Replication interval time is 30 minutes. This model with a centralized WINS server communicating with the other WINS servers is called the hub-and-spoke model is the only proposed solution where replicated information from one WINS server reaches all the others within 2 replications, which would be less than 60 minutes. In this model replication passes through the central WINS server from the one WINS server to all the other WINS servers.

Incorrect Answers:
A: With the WINS server in a circular arrangement it would take at least four replications for the WINS information to reach the WINS server farthest away in the circle. This would make replication time of around 2 hours.
C: WINS server cannot be configured to automatically configure the other WINS servers as push/pull partners. The replication must be manually configured on the WINS servers.
D: The WINS servers need to be configured as replication partners.

QUESTION NO: 54
You are the administrator of TestKing's network. The network consists of a single IP subnet that uses DHCP to automate client computer configuration. You install a WINS server on the network to reduce broadcast traffic for name resolution.

After several days, users report that the network response time is still unacceptably slow. You investigate and discover that the levels of broadcast traffic have not been reduced. When you view the WINS database, you also find that the only entry is for the WINS server itself.

What should you do to resolve this problem?

    A.   Configure the WINS server as a DHCP client computer
    B.   Configure the DHCP server as a WINS client computer
    C.   Configure a DHCP scope option to include the address of the WINS server
    D.   Configure static mappings on the WINS server for each client computer
    E.   Configure a reservation in the DHCP scope for the WINS server.

Answer: C
Explanation: In addition to an IP address, DHCP servers can be configured to provide optional data to fully configure TCP/IP for clients. In this scenario we configure the DHCP scope option to include the IP address of the WINS server. The next time the clients contacts the DHCP server they will be configured to use the WINS server. To accomplish this we must select the DHCP console in the Administrative Tools, open Scope, Right-click Scope options, select Configure Scope, and enable 044 WINS/NBNS Servers and enable 46 WINS/NBT Node Type.

Incorrect Answers:
A: The WINS server should have a static IP address, it should not be a DHCP client.
B: The DHCP server does not need to be configured to be a WINS clients, it must configure the address of the WINS server in the scope option.
D: It is not necessary for static mapping on the WINS server. The DHCP server must be configured to include the WINS server address in the scope option.
E: A reservation in the DHCP scope for the WINS server would only ensure that the WINS server uses the same IP addresses. It would not enable the clients to use the WINS server.

QUESTION NO: 55
You are the administrator of a Windows 2000 network The network has three Windows 2000-based WINS servers named Srv1, Srv2, and Srv3. You want to periodically compact the WINS database to reclaim unused space.

How should you perform a manual compaction of the WINS database on the Srv1 WINS server?

    A.   Configure the Srv1 WINS server to block replication of WINS records from the Srv2 and Srv3 WINS servers.
               Initiate database consistency checking.
               Allow replication of records from the Srv2 and Srv3 WINS servers.
    B.   Stop the Srv1 WINS server.
               Use the jetpack command-line tool to compact the WINS database.
               Start the Srv1 WINS server again.
    C.   Stop the Srv1 WINS server.
               Use the **Backup Database** command to create a backup of the Srv1 WINS database.

Compact the backup of the database by using the compact command-line tool.
Use the **Restore Database** command to restore the backup of the database. Start the Srv1 WINS server again
D.　　In the WINS console, use the **Scavenge Database** command

Answer: B
Explanation: To compact a WINS database we must stop the WINS server service. Then at the command prompt we must issue the jetpack wins.mdb tmp.mdb command and then restart the WINS server service.

Incorrect Answers:
A:　WINS replication configuration or database consistency checking are not used when the WINS database should be compacted.
C:　The compact command is used to compress files in general not to compact the WINS database.
D:　The Scavenge database command is used to remove stale records from the WINS database. It is not used to compact the WINS database.

QUESTION NO: 56
You are the administrator of a Windows 2000 network. The network has six Windows 2000-based WINS servers and two Windows 2000-based DHCP servers.

To anticipate the migration of the network from WINS to DNS, you decide to remove one WINS server named Wins6 from the network by performing the following actions.

- **On Wins6, stop the WINS Service and uninstall WINS.**
- **On the DHCP servers in the network, reconfigure the options to no longer specify Wins6 as a WINS server Configure the DHCP options to instead use the other five WINS servers equally.**
- **On WINS client computers that are manually configured to use TCP/IP, reconfigure the network properties to no longer use Wins6 as a WINS server Configure these client computers to instead use any of the other five WINS servers.**
- **On one of the remaining WINS servers, delete the static mappings originally made on Wins6.**

After two weeks, you notice that static mappings originally made on Wins6 are still present on all the remaining WINS servers.

What should you do to permanently remove these unwanted static mappings from the remaining WINS servers?

A.　　On the remaining WINS servers, use the **Scavenge Database** command in the WINS console
B.　　On the remaining WINS servers, perform an offline compaction of the WINS database
C.　　Configure the remaining WINS servers to use Migrate On handling of static entries
D.　　On one of the remaining WINS servers. Manually tombstone the Wins6 owner from the database.

Answer: D
Explanation: By manually tombstone the records which belonged to the Wins6 WINS server, the tombstone information will replicate to other WINS servers and the corresponding records will be tombstoned on the other WINS servers as well. The tombstone records will eventually be deleted.

Incorrect Answers:
A: Scavenging the database would only remove stale records, not the static mappings.
B: Offline compacting of the WINS database would not remove any wins records.
C: The migrate on setting would enable static entries in the WINS database to be challenged and dynamically updated by clients. This would not remove any static mappings which will not be challenged though.

QUESTION NO: 57
You are the administrator of a Windows 2000 network. The network has two Windows 2000-based WINS servers. You want periodic backups of the WINS database of both WINS servers to occur automatically.

How should you configure the network to accomplish this goal?

A.   In the WINS console on both WINS servers, use the right mouse button (Right-click) to select the server name, and then select the **Back Up database** command.
B.   In the WINS console on both WINS servers, configure the general properties of the WINS server to specify a default backup path.
C.   On both WINS servers, use Windows backup to schedule a regular backup of the system32\Wins folder.
D.   On the both WINS servers, configure the File Replication Service to copy the System32\Wins folder to another location on the disk.

Answer: B
Explanation: Once a backup folder for the database has been specified, WINS performs a complete WINS database backup every three hours.

Incorrect Answers:
A: Manually backing up the WINS database will not schedule any period WINS backups for the future.
C: The Windows backup cannot be used to backup the WINS database. The WINS console must be used to specify the default backup directory.
D: The WINS database cannot be backed up by the file replication service. WINS database backups must configured from the WINS console.

QUESTION NO: 58
You are the administrator of TestKing's network. The network consists of four IP subnets connected by a router. The network contains 12 Windows 2000 Server computers and 100 Windows 2000 Professional computers, evenly distributed across the four subnets. All of the servers are used to server file and print resources to the client computers.

You install the WINS server service on one server on one subnet. You configure the WINS option in a DHCP scope to configure all of the other computers on the network to register with and query the WINS server for NetBIOS name resolution.
Within four hours of the installation and configuration, users on the remote subnets report that they cannot access resources located on the WINS server by NetBIOS name. Other TCP/IP connectivity is not affected. Users located on the same subnet as the WINS server are experiencing no problem accessing these same resources.

What should you do to resolve this problem?

    A.   Install a WINS proxy agent on each remote subnet.
    B.   Install a WINS proxy agent on same subnet as the WINS server.
    C.   Configure the WINS server to include IP addresses of each gateway on the router.
    D.   Configure the WINS server to include its own IP address as a WINS client computer.

Answer: D
Explanation: The clients receive their WINS Server address, along with other IP configuration information, from the DHCP server. But they cannot use the NetBIOS name of the WINS server to access resources on the WINS server as the WINS server must also be configured as WINS client.

Incorrect Answers:
A: WINS proxy agent is only useful for non WINS-clients.
B: WINS proxy agent is only useful for non WINS-clients.
C: The DHCP server scope option is configured to include a default gateway address. WINS is only used for NetBIOS to IP address name resolution.

QUESTION NO: 59
You are the administrator of TestKing's network. Your network has 1,900 hosts. Your network requires Internet connectivity. Aside from the connection to the Internet, your network is not routed. Your Internet service Provider (ISP) assigns you the following eight network addresses:

    192.24.32.0/24
    192.24.33.0/24
    192.24.34.0/24
    192.30.35.0/24
    192.30.36.0/24

192.30.37.0/24
192.30.38.0/24
192.30.39.0/24

You want to minimize the complexity of routing tables on the network while maintaining Internet connectivity for all hosts. Which subnet mask should you configure to meet these goals?

    A.   255.255.240.0
    B.   255.255.248.0
    C.   255.255.252.0
    D.   255.255.254.0
    E.   255.255.255.0

Answer: B
Explanation: There must be 1,900 clients on the subnet. At least eleven bits must be used for these 1,900 hosts, since 2**11=2048 and not 10 bits since 2**10 = 1024. This leaves 21 (32-11) bits for the subnet mask.
Subnet mask in binary: 11111111.11111111.11111000.00000000
Subnet mask in decimal: 255.255.248.0

Incorrect Answers:
A: The subnet mask 255.255.240.0, is not appropriate for the 8 subnets provided by the ISP.
C: The subnet mask 255.255.252.0, or in binary
        11111111.11111111.11111100.00000000, leaves 10 bits for the hosts, which translates to 1024 host which is not enough.
D: The subnet mask 255.255.254.0, or in binary
        11111111.11111111.11111110.0, only leaves 9 bits for the hosts, which translates to only 512 hosts but 1,900 hosts are required.
E: The subnet mask 255.255.255.0, or in binary
        11111111.11111111.11111111.0, only leaves 8 bits for the hosts, which translates to only 256 hosts but 1,900 hosts are required.

QUESTION NO: 60
Your company has a Simple Network Management Protocol (SNMP)-enabled network router installed on its network. Your company wants to monitor all SNMP traffic generated by the router. You install Network Monitor on Windows 2000 server computer on your network.

Your router is configured to trap to an SNMP Manager installed on another server. You want to receive a notification whenever router raises an SNMP trap.

What should you do? (Choose two)

    A.   Create a Network Monitor filter that has a pattern match for SNMP traffic.

Leading the way in IT testing and certification tools, www.testking.com

B.   Install SNMP on the server.
C.   Create a network monitor trigger to run the **Net Send** command.
D.   Create a TCP/IP filter on the server.
E.   Start the Windows 2000 Alerter Service on the server.
F.   Configure the network router to trap to the IP address of the server.

Answer: A, C
Explanation: First a Network Monitor filter selects only the frames that has a pattern match for SNMP traffic. Then A network monitor trigger has to be configured to trigger on Pattern match for SNMP traffic, and to run a net send command which will notify you on the SNMP trap.

Incorrect Answers:
B: SNMP is already installed on a Windows 2000 Server. Only one SNMP server is needed.
D: A Network monitor filter, not a TCP/IP filter on the server, will catch the SNMP trap message.
E: The alerter service must be running, and it is enabled by default, so that the net send command will be allowed to reach you.
F: The router is, by default, already configured to trap SNMP events. These traps are broadcasts so the IP address of the SNMP server does not have to be configured.

QUESTION NO: 61
You are the administrator of a Windows 2000 network that has a main office and one branch office. The company leases a 128-Kbps ISDN line to connect the main office to the branch office. You configure Routing and Remote Access on a stand-alone Windows 2000 server computer in each office to provide a demand-dial connection.

You want to encrypt traffic over the ISDN connection, and you want to prevent unnecessary connections over the ISDN line.

What should you do?

A.   Configure a PPTP demand-dial connection to connect the two offices over the ISDN connection and ensure that data encryption is enabled.
         Set the demand dial filters to exclude NetBIOS broadcast traffic.
B.   Configure a PPTP demand-dial connection to connect the two offices over the ISDN connection and ensure that data encryption is enabled.
         Set the IP Demand Dial Filters to exclude Remote Procedure Call traffic.
C.   Configure an L2TP demand-dial connection to connect the two offices over the ISDN connection.
         Configure inbound and outbound filters to exclude all NetBIOS broadcast traffic.
D.   Configure an L2TP demand-dial connection to connect the two offices over the ISDN connection.
         In the demand dial filter list, configure filters to exclude Remote Procedure Call traffic.

Answer: A
Explanation: PPTP demand dial-in connection which is configured to enabled data encryption will encrypt all traffic. Furthermore, by configuring the demand dial filters to exclude NetBIOS broadcasts would prevent some unnecessary name resolution traffic over the ISDN line.

Incorrect Answers:
B: The demand dial filters should be configured to exclude NetBIOS broadcasts not Remote Procedure Call traffic.
C: L2TP must be used with IPSec to encrypt data.
D: L2TP must be used with IPSec to encrypt data.

QUESTION NO: 62
You are the administrator of TestKing's network. Your network consists of 100 computers that use the IPX/SPX protocol. You plan to migrate the network to use TCP/IP and establish connectivity within the network. Your Internet Service provider (ISP) assigns the address 192.168.16.0/24 to your network.

Your network requires 10 subnets with at least 10 hosts per subnet. Which subnet mask should you configure to meet this requirement?

    A.   255. 255. 255. 0
    B.   255. 255. 255. 192
    C.   255. 255. 255. 224
    D.   255. 255. 255. 240
    E.   255. 255. 255. 248

Answer: D
Explanation: 10 hosts in each subnet require four bits to the hosts which would supply 14 hosts (2**4-2). The remaining 28 bits (32-4) could be used for the network mask.
Network mask, in binary: 11111111.11111111. 11111111.11110000
Network mask, in decimal: 255.255.255.240
Subnetting would be given 4 hosts bits (32-24-4) which give 14 subnets (2^4-2) which is more than required 10.

Note: To calculate the number of available host we use the formula: 2^(number of host bits)-2. We must subtract the lowest address since it is a network address, and the highest address since it is the network broadcast address.

Incorrect Answers:
A: A network mask of 255.255.255.0 gives 254 hosts, but no bits for subnet. 10 subnet is required.
B: A network mask of 255.255.255.192 gives 64 hosts, but only 2 subnets (10 required).
C: A network mask of 255.255.255.224 gives 32 hosts, but only 6 subnets (10 required).
E: A network mask of 255.255.255.248 gives 6 hosts, but 10 is required.

QUESTION NO: 63
You are the administrator of TestKing's network. Your network consists of Windows 2000 server computer and Windows 2000 Professional computers.

You create an IPSec policy named accountingsec for use by employees in your accounting department. Your company is concerned that the keys used for encryption could be compromised and used to decrypt future communications.

You want to prevent the re-use of previous-session keys. You also want to limit performance degradation. What should you do?

    A.   Decrease the frequency of policy checks for updates.
    B.   On the **Generate a new key every** property, modify the time allocations.
    C.   Select the **Master key Perfect Forward Secrecy** check box.
    D.   Select the **Session key Perfect Forward Secrecy** check box.

Answer: D
Explanation: Session Key Perfect Forward Secrecy creates a new master key during every session rekey operation and is the most secure setting.

Incorrect Answers:
A: Decreasing the frequency of policy checks would not prevent use of previous session keys.
B: If the time allocations of the **Generate a new key every** property is configured, a re-authentication and new key generation at that interval would be configured. But there is no guarantee that a new session will not use a previous session key.
C: Master key PFS should be used with caution as it requires re-authentication. This may cause additional overhead for any domain controllers in your network.

QUESTION NO: 64
You are the administrator of a Windows 2000 network. You administer the routers in your network. Your Internet Service Provider (ISP) has assigned your network the network ID 172.24.8.0/22. You assign blocks of IP addresses to other administrators in your company when they request them.

All of the routers in your network use either Open Shortest Path First (OSPF) or RIP version 2. You want to create two subnets that will each have approximately 75 computers. Your company expects the number of computers on these subnets to remain at 75.

To create the subnets that will accommodate 75 computers, you want to use the most specific number of bits in your subnet mask. You also want to use the first two available network ID numbers.

For the two subnets you need to create, click the Select and Place button, and then drag the appropriate network ID numbers to the appropriate boxes.

SELECT AND PLACE

Possible Network ID Numbers

Select from these items

172.24.8.0/22

Place ID Number here

Router

Place ID Number here

172.24.12.0/22

172.24.16.0/22

172.24.24.0/22

172.24.8.128/25

172.24.9.0/25

172.24.16.0/25

Answer:

Possible Network ID
Numbers

Select from these items

172.24.8.0/22

172.24.8.128/25

172.24.12.0/22

172.24.16.0/22

172.24.9.0/25

Router

172.24.24.0/22

172.24.16.0/25
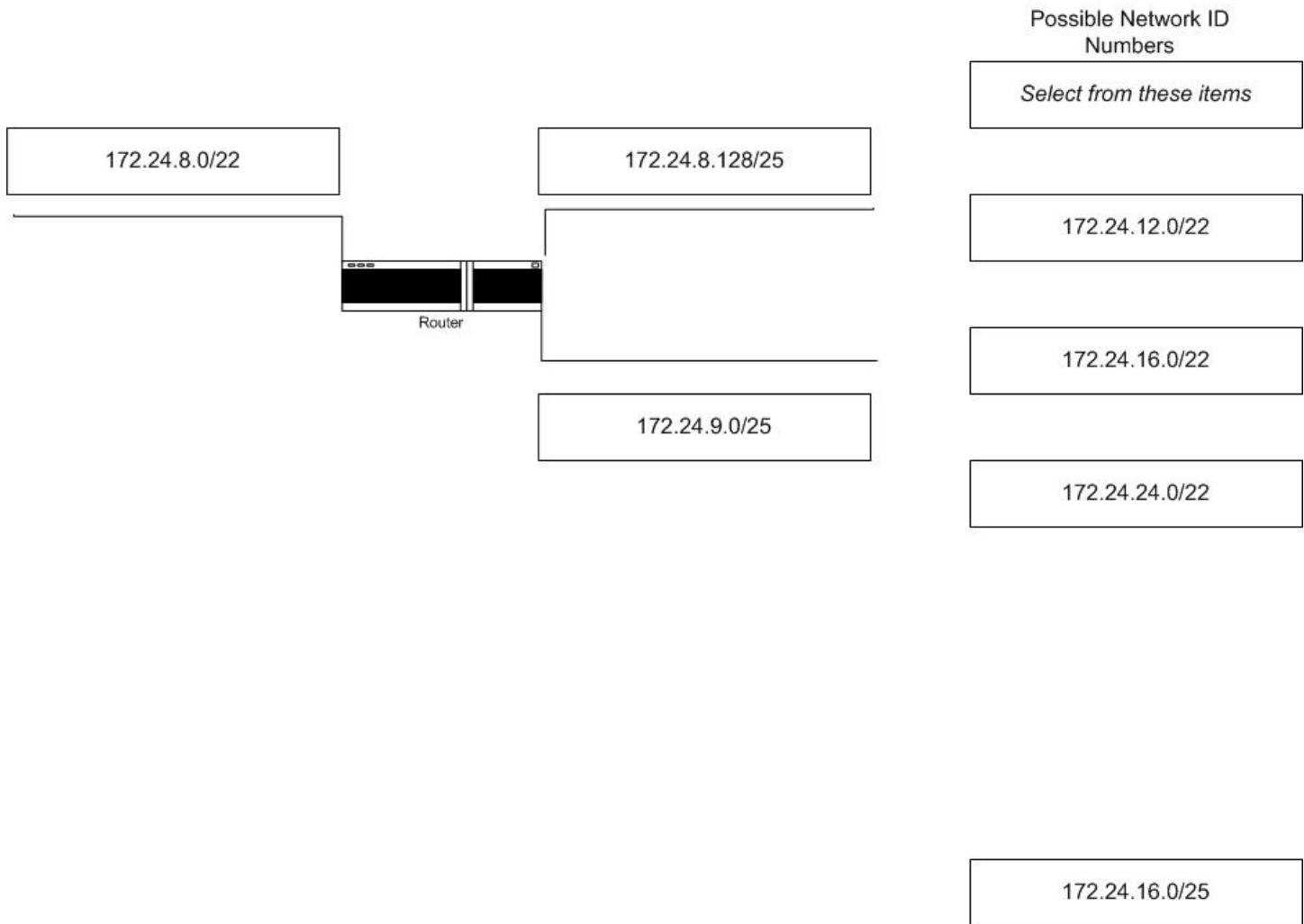
172.24.8.128/25
172.24.9.0/25

Explanation: 75 hosts would require 7 bits (2**7=128, 2**6=64), which leaves 25 bits (32-7) for the subnet mask.
The two most specific subnets with a subnet mask of 25 bits and a network ID 172.24.8.0 are:
Most specific: 172.24.8.0 + 0.0.0.128 = 172.24.8.128
Next most specific: 172.24.8.0 + 0.0.1.0 = 172.24.9.0

Incorrect Answers:
172.24.12.0/22: 25 bits should be used for the network mask
172.24.16.0/22: 25 bits should be used for the network mask
172.24.24.0/22: 25 bits should be used for the network mask
172.24.16.0/22: this is not the two most specific subnet IDs of 172.24.8.0/22

Leading the way in IT testing and certification tools, www.testking.com

QUESTION NO: 65
You are the administrator of TestKing's network. Your network consists of 15 Windows 2000 Server computers, 100 Windows 2000 Professional computers, and one Netware server. Your users need to access the Sys:volume on the Netware server. You want TestKing's administrators to have complete access to the Sys:volume. You want all others users to have read-only access.

You configure gateway service for Netware on a Windows 2000 Server computer. You want to configure the appropriate access to the Netware server.

What should you do? (Choose Two)

A.   To the NTGateway Group on the NetWare server, add the users accounts that need access to the Netware server.
B.   To the NTGateway group on the Windows 2000 server computer, add the user accounts that need access to the Netware server.
C.   To the NTGateway group on the Netware server, add the NTGateway user account.
D.   To the NTGateway group on the Windows 2000 server computer, add the NTGateway user account.
E.   On the Windows 2000 Server computer, grant Full Control permission to administrators and Read permissions to the users.

Answer: C, E
Explanation: The NTGateway group should be created at the NetWare server not at the Windows 2000 Server. A Netware user account, with the necessary rights for the resources that you want to access, must be a member of the NTGateway group on the Netware server.
On the computer running Windows 2000 Server and acting as a gateway, you can set share-level permissions for each resource made available through the gateway. In our case: Full Control to administrators and Read permissions to users.

Incorrect Answers:
A: Only one single NetWare user account must be added to the NTGateway group on the NetWare server.
B: The NTGateway group should be created at the NetWare server not the Windows 2000 server computer.
D: The NTGateway group is created on the NetWare server not the Windows 2000 Server computer.

QUESTION NO: 66
You are the administrator of you company's network. The network is configured as shown in the exhibit.
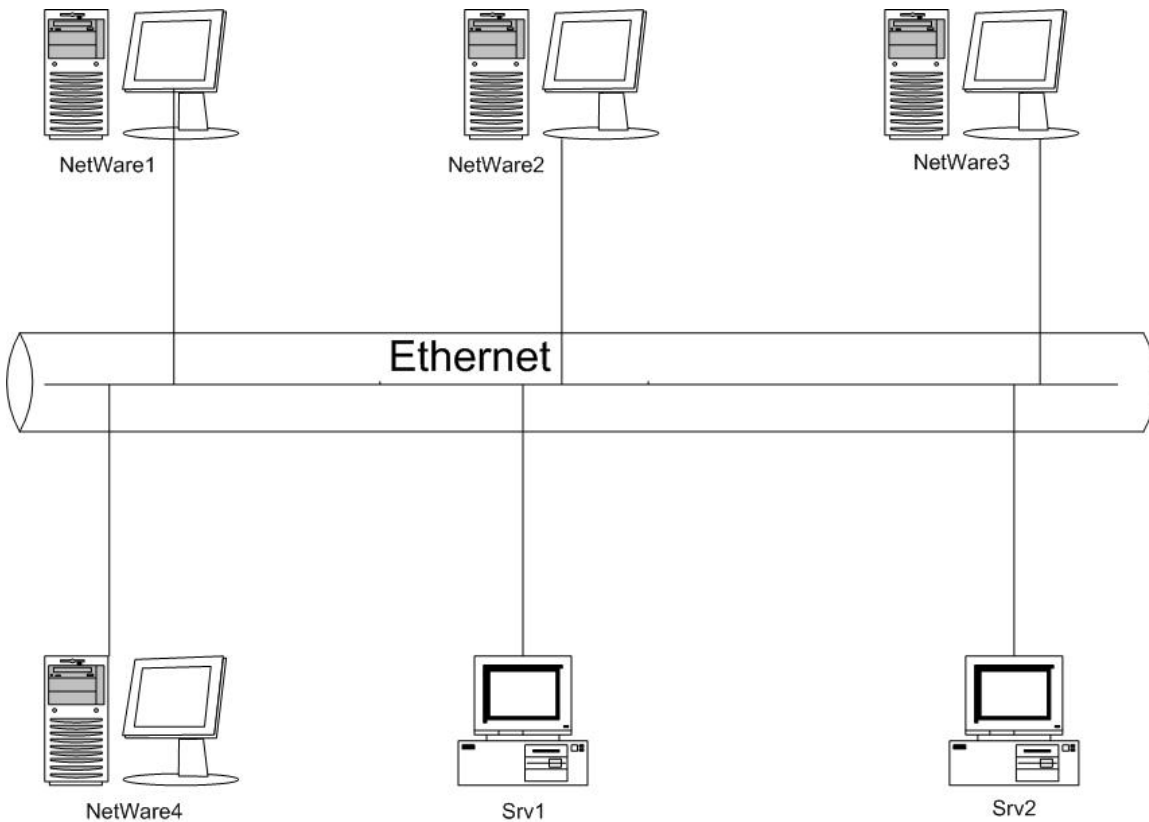
On you Windows 2000 Server computer named Srv1, you install client service on NetWare and NWLink
with default settings. You perform these installations to access files stored on TestKing's NetWare
servers. From the Srv1 you can connect Srv2. You can also connect to NetWare1 and NetWare3, but you
cannot connect to NetWare2 and NetWare4. NetWare2 and NetWare4 run different versions of NetWare
than NetWare1 and NetWare3.

You want to configure Srv1 to connect to all the NetWare servers. What should you do?

A.   Set the adapter to **Manual frame type detection** and add the frame type of each NetWare server.
B.   Manually configure the internal network number to 00000000.
C.   Enable direct hosting of the Internet work packet exchange (IPX).
D.   Install file and print services for the NetWare.

Answer: A
Explanation: On this network two different NWLink frame types are used. On Windows 2000 computers
NWLink automatically detects the frame type used by the network adapter. If multiple frame types are detected,
NWLink sets the frame type to 802.2. If more than one frame type must be supported the additional frame types
must be added manually. This is done by the following steps on a Windows 2000 Server computer:
Open Network and dial-up connections, Right click appropriate interface, select Properties, select NWLink,
select Properties, select Manual frame type detection, choose Add and Select appropriate Frame Type.

Leading the way in IT testing and certification tools, www.testking.com

Note: this setting could also be accomplished by editing the registry: add both types to the multi-string value PktType in
 HKLM\SYSTEM\CurrentControlSet\Services\NwlnkIPX\Parameters\Adapters\<ID>, where <ID> is the network adapter identifier

Incorrect Answers:
B: Internal network number must be used to run FPNW or IPX routing. It is not used to support different NWLink frame types.
C: Direct hosting is a feature that allows computers to communicate over IPX, bypassing the NetBIOS layer. It is not used to support multiple frame types.
D: File and Print Services for NetWare (FPNW) is used to provide NetWare client access to file and print resources on a computer running Windows 2000 Server, it is not used to support different NWLink frame types.

QUESTION NO: 67
You are the administrator of the blueskyairlines.com domain. You maintain a local DNS server to provide name resolution within your Internet domain. Your DNS server runs on Windows 2000 server. You have five web servers, which contain company and flight information in addition to the online flight reservation system.

For load-balancing purposes, each web server is configured to maintain exactly the same contents as all the other web servers. All the web servers respond to the host name www.blueskyairlines.com. Customer feedback indicates that web server response times are unacceptably slow. You monitor your web servers and discover that only one of the five servers is servicing customer requests, while the others are sitting idle.

You want to ensure load balancing and improve response time for customer web request. What could you do in the DNS management console? (Choose two)

A.   Enable round robin in the DNS server's properties.
B.   Disable round robin in the DNS server's properties.
C.   Enable forwarders and configure them to point to each web server.
D.   Verify that A (host) records have been created for each web server.
E.   Verify that CNAME (canonical name) records have been created for each web server.

Answer: A, D
Explanation: Round robin is an approach for performing load balancing. It's used to share and distribute the network resource load. With round robin, the host name contained in a query, for which multiple RRs exist, are rotated each time the query is answered.
In this scenario five host (A) records for www.blueskyairlines.com (pointing to the different web servers) must be created.

Incorrect Answers:
B: To ensure load balancing and to improve performance Round robin must be enabled, not disabled.
C: Forwarders is used to forward DNS name queries to other DNS servers. It can not be used to load balance the web servers.
E: CNAME records define aliases for resources. It can not be used to increase performance of the Web servers. Instead host (A) records with identical names but different IP addresses must be created for the Web servers.

QUESTION NO: 68
You are the administrator of a Windows 2000 network. Your internal DNS server is located behind a firewall. When you test your DNS server by using the Monitoring tab on the server's properties page, the DNS server passes the simple test but fails the recursive test.

What could you do to resolve the problem?

  A.   Run the **ipconfig/ registerdns** command.
  B.   Delete the *Systemroot*\system32\dns\cache.dns file.
  C.   Copy the *systemroot*\system32\dns\samples\cache.dns file to the *systemroot*\system32\dns\cache.dns file.
  D.   Create a forward lookup zone for the root zone. Name the forward lookup zone ".".
  E.   Create a reverse lookup zone for the subnet on which the resource records for the primary name server are located.

Answer: C
Explanation: The recursive test fails. No forwarders are used. The internal DNS server must be configured with forwarders to be able to resolve external addresses. One likely cause is a root hints problem. By replacing the cache.dns file the root hints will be replaced and the internal DNS server will be able to use external DNS server as forwarders.

Reference:
Replacing Root Hints with the Cache.dns File (Q249868)
HOW TO: Configure DNS for Internet Access in Windows 2000 (Q300202)

Incorrect Answers:
A: ipconfig/registerdns would register the computer, the DNS server, in DNS. This does not apply to the problem at hand.
B: Cache.dns contains the addresses of DNS's root servers. Deleting it would cause damage to the DNS Server.

Leading the way in IT testing and certification tools, www.testking.com

D: Creating a new empty root zone would make the internal DNS server a root server. It would never use any forwarders. Only local name resolution would be possible.
          Deleting an empty root zone, not creating one, could be helpful in this scenario.
E: Create a new reverse lookup zone, would enable IP to name resolving, but would not fix the current DNS problem.

QUESTION NO: 69
You are the administrator of one standard primary DNS server and two standard secondary DNS servers in a Windows 2000 domain. There are no other DNS servers on the network. The domain includes Windows 2000 Professional computers and a Windows 98 computer.

The DNS zone for the Windows 2000 domain is configured to allow dynamic updates. All three DNS servers are located on domain controllers. You want client computers to be able to register with any DNS server.

What should you do?

    A.   Change the zone type of the DNS zone for the Windows 2000 domain on all three DNS servers to active directory integrated.
    B.   Change the settings on the standard primary DNS server to notify the two standard secondary DNS servers when the zone is updated.
    C.   Change the settings on the standard primary DNS server to allow zone transfers to only the two standard secondary DNS servers.
    D.   Change the dynamic update option on the standard primary DNS server to allow only secure updates.

Answer: A
Explanation: With primary and secondary servers, the clients can only be registered at the primary server. With three Active Directory DNS Servers the clients could register themselves dynamically on any of them.

Incorrect Answers:
B: Configuration of notification concerns zone transfers and does not change the way clients register themselves.
C: Zone transfers will not make the clients able to register themselves dynamically at any server.
D: Only secure updates can only be configured in Active Directory Integrated zones.

QUESTION NO: 70
You are the administrator of Windows 2000 network. You have three Windows 2000 domain controllers in a single domain. Your primary DNS server is installed on a domain controller named dc1.contoso.com.

You have two secondary DNS server installed on member servers named srv1.contoso.com and srv2.contoso.com.

You want to increase fault tolerance for your DNS infrastructure. You also want to optimize and simplify the management of replication and zone transfers on your network.

How should you accomplish these goals?

    A.   Promote the member servers that are hosting the DNS server to domain controllers.
    B.   Add srv1.contoso.com and srv2.contoso.com to the notify list on the primary DNS server.
    C.   Remove the DNS server service from the member servers. Install the DNS server service on the domain controller. Convert the zone hosted by dc1.contoso.com to an Active Directory Integrated zone.
    D.   Set the Time to Live (TTL) value in the SOA (start of authority) record on the primary DNS server to a low value.

Answer: C
Explanation: By removing the secondary DNS servers, installing DNS on a Domain controller, and converting the zone to Active Directory-integrated zone we would increase fault tolerance, since every DNS server has a full updateable replica of the DNS zone, optimize zone replication since incremental zone transfers instead of full zone transfers could be performed, simplify replication management: replication is integrated in the Active Directory replication process and does not have to be configured.

Incorrect Answers:
A: Only promoting the member servers to domain controllers would not increase fault tolerance, optimize zone replication or simply replication management since the zones still would be secondary zones.
B: Adding srv1.contoso.com and srv2.contoso.com to the notify list will make the records on the secondary servers more up to date, but it would not increase fault tolerance, optimize zone replication or simply replication management since the zones still would be secondary zones.
D: By setting the TTL value on the SOA record on the primary server to a low value would keep DNS records more current at the secondary servers, but would not increase fault tolerance, optimize zone replication or simply replication management since the zones still would be secondary zones.

QUESTION NO: 71
You are the administrator of TestKing's network. Your network is configured as shown in the exhibit.
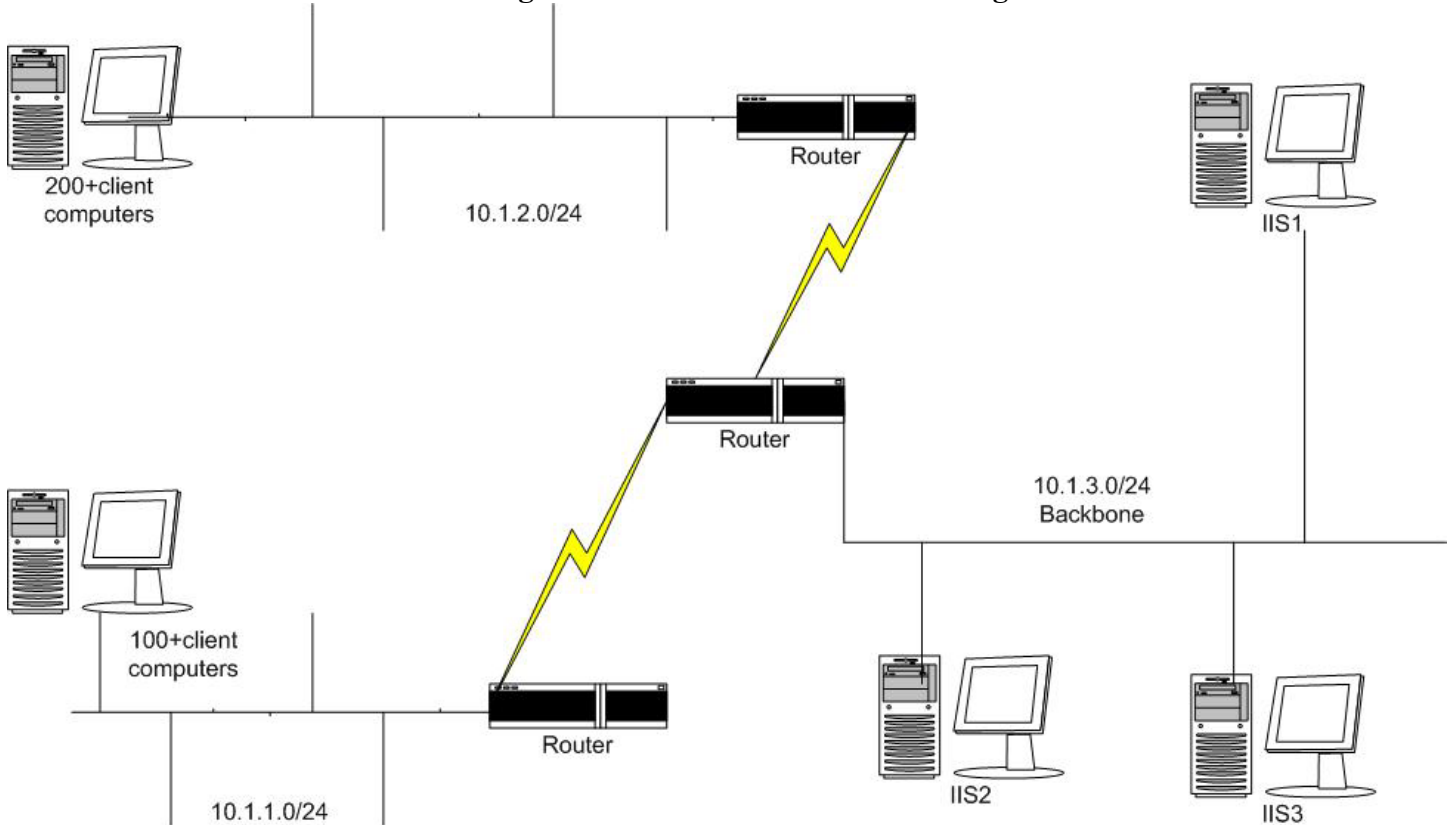
Your company has an intranet web application named appz that utilizes resources on Internet Information Services (IIS).

For performance reasons, your company mirrors the content of appz on three web servers: IIS1, IIS2 and IIS3. You want to configure your network to allow access to the other web servers in the event of failures. You want to configure DNS by using the fewest possible resources.

What should you do?

A.   Configure one DNS server so that it has one DNS zone.
        Enable Round Robin.
        Create an A (host) record for appz for each web server's IP address.
B.   Configure one DNS server so that it has one DNS zone.
        Disable Round Robin.
        Create an A (host) record for appz for each web server's IP address.
C.   Configure three DNS servers so that each has one DNS zone.
        Enable Round Robin.
        Add an A (host) record for appz for each web server on each DNS server.

D.   Configure three DNS servers so that it has one DNS zone.
        Disable Round Robin.
        Add an A (host) record for appz for each web server on each DNS server.

Answer: A
Explanation: Round robin is an approach for performing load balancing. It is used to share and distribute the network resource load. With round robin, the host name contained in a query, for which multiple RRs exist, are rotated each time the query is answered. Round Robin also provides redundancy. In this scenario three host (A) records for appz (pointing to IIS1, IIS2 and IIS3 respectively) must be created. These three host (A) records must be added to the same DNS zone to provide load balancing and redundancy.

Incorrect Answers:
B: To ensure load balancing and to improve performance Round robin must be enabled, not disabled.
C: With three host (A) records in different zones the name resolution would not be able to rotate between IIS1, IIS2 and IIS3; we would not have any load balancing or redundancy.
D: To ensure load balancing and to improve performance Round robin must be enabled, not disabled.

QUESTION NO: 72
You are the administrator of a Windows 2000 network. The network consists of a Windows 2000 Server computer named Atlanta and 120 Windows 2000 Professional computers. Atlanta has a dial-up connection that connects to the Internet.
All Windows 2000 Professional computers on the network are configured to use a dynamically assigned IP address. The network has one DHCP server.

To allow all Windows 2000 Professional computers on the network to access the Internet through the dial-up connection of Atlanta, you install and configure the Network Address Translation (NAT) routing protocol on Atlanta.

Your Internet service provider (ISP) has allocated four IP addresses, 207.46.179.4 through 207.46.179.7 to your network.

You want Atlanta to use the four IP addresses for the translated connection to the ISP. How should you configure Atlanta?

A.   Configure the Nat routing protocol to use the IP addresses in the range starting with 207.46.179.4 with a mask of 255.255.255.252 for the DHCP Allocator.
B.   Configure the public interface of the NAT routing protocol to use an address pool with a starting address of 207.46.179.4 and a mask of 255.255.255.252
C.   Configure the LAN interface of the NAT routing protocol to use an address pool with a starting address of 207.46.179.4 and a mask of 255.255.255.252
D.   Configure the NAT routing protocol to use special ports on the public interface. Use private addresses 207.46.179.4 through 207.46.179.7

Answer: B
Explanation: By configuring the public interface of the NAT protocol with the public IP addresses provided by the ISP the NAT would be set up correctly. A subnet mask of 255.255.255.252 is also correct; as it allows 4 public addresses.

Incorrect Answers:
A: The DHCP allocator functionality in NAT enables all DHCP clients in the network to automatically obtain an IP address, subnet mask, default gateway, and DNS server address from the NAT computer. The DHCP allocator uses private addresses on the internal LAN interface, not public addresses like 207.46.179.4.
C: Public addresses, like 207.46.179.4, cannot be exposed on the internal LAN interface.
D: Special ports could be used to make private resources on the LAN available for internet users. This is done by a mapping public address to a private address with a special port. The public addresses 207.46.179.4 through 207.46.179.7 cannot be used at private addresses.

QUESTION NO: 73
You are the administrator of a Windows 2000 network. The network consists of a Windows 2000 Server computer named ServerA and 45 Windows 2000 Professional computers. ServerA has a dial-up connection that connects to the internet.

To allow all Windows 2000 Professional computers on the network to access the internet through dial-up connection of ServerA, you install and configure the Network Address Translation (NAT) routing protocol on ServerA.

All Windows 2000 Professional computers in the network are configured to use Automatic Private IP Addressing (APIPA). There is no DHCP server on the network.

You want to configure the network to use IP addresses in the range of 172.16.65.1 through 172.16.65.250 for ServerA and the 45 Windows 2000 Professional computers.

What should you configure ServerA to accomplish this goal? (Choose all that apply)

  A.   Assign an IP address 172.16.65.1 to the LAN interface of ServerA.
  B.   Enable Internet Connection Sharing on the dial-up connection of ServerA.
  C.   Configure Routing and Remote Access on ServerA to automatically assign IP addresses in the range of 172.16.65.2 through 172.16.65.250 dial-in client computers.
  D.   Configure the NAT routing protocol on ServerA to automatically assign IP addresses in the range of 172.16.65.2 through 172.16.65.250 to computers on the private interface.
  E.   Configure the public NAT interface to use an IP address pool in the range of 172.16.65.2 through 172.16.65.250.

Answer: A, D
Explanation: The LAN interface of the server should assigned the first IP address in the range of 172.16.65.1 through 172.16.65.250; namely 172.16.65.1.
The NAT computer must be set up to automatically assign IP addresses, in the 172.16.65.2 through 172.16.65.250 range, to the local computers.

Incorrect Answers:
B: Internet Connection Sharing (ICS) is not needed here, since NAT has already been installed.
C: This is a dial-up connection to Internet which uses NAT, not a dial-in connection using RRAS. So there is no point to configure the Server to automatically assign IP-addresses to dial-in clients. The scenario does not mention dial-in clients or RRAS in any way.
E: The public NAT interface cannot use private IP addresses in the range of 172.16.65.2 through 172.16.65.250.

QUESTION NO: 74
You are the administrator of a Windows 2000 network. The administrator of TestKing's Human Resources Organizational Unit wants to be able to manage Encrypting File System for the users in their department. The administrators of the human resources department belong to a group named HRAdmins, which has full administrative privileges to the OU.

To make it possible for the members of HRAdmins to manage EFS for the users in their department, you install an Enterprise Certificate Authority for use by the entire company. However, the administrators of the human resources department notify you that they are unable to create a Group Policy that allows them to manage EFS for their department.

What should you do to enable the administrators of the Human Resources Organizational Unit to create a Group Policy to manage EFS for the users in their department? (Choose Two)

   A.   Install a Subordinate Enterprise CA for use by the human resources department.
   B.   In the certification Authority console for the CA, add a new policy setting for a EFS Recovery Agent certificate.
   C.   In the certification authority console for the CA, add a new policy setting for a Basic EFS certificate.
   D.   In Active Directory sites and services, grant the Enroll permission to the HRAdmins for the Enrollment Agent Certificate Template.
   E.   In Active Directory sites and services, grant the Enroll permission to the HRAdmins for the EFS Recovery Certificate Template.
   F.   In Active Directory sites and services, grant the Enroll permission to the HRAdmins for the EFS Certificate Template.

Answer: B, E

Explanation: The administrators of the Human Resources department must be set up as Recovery Agents in order to be able to administer EFS for their department. This can be accomplished by adding a new policy setting for an EFS Recovery Agent certificate in the appropriate CA and granting the Enroll permission to the HRAdmins for the EFS Recovery Certificate Template in Active Directory sites and services.

Incorrect Answers:
A: It is not necessary to install a subordinate Enterprise CA. The Enterprise CA can very well be used.
C: A new policy setting for a EFS Recovery Agent certificate, not a Basic EFS certificate, should be added.
D: The HRAdmins should be granted enroll permissions to the EFS Recovery Certificate Template not the Enrollment Agent Certificate Template.
F: The HRAdmins should be granted enroll permissions to the EFS Recovery Certificate Template not the EFS Certificate Template.

QUESTION NO: 75
You are the administrator of a Windows 2000 network. Your Public Key Infrastructure consists of an offline Certificate Authority (CA) and a number of subordinate CAs.

Your company is selling one of its divisions. This division has a subordinate CA that it uses to issue certificates. You want to ensure that once the division is sold, applications and other CAs on your network will not accept the former division's certificates. You also want to ensure that you can implement your solution by using a minimum amount of administrative effort.

What should you do?

A. On the division's subordinate CA, revoke all the certificates it has issued. Publish the Certificate Revocation List (CRL) to a server on your network. Uninstall the CS software and remove the CS files.
B. On the company's root CA, revoke the certificate of the division's subordinate CA. Publish the Certificate Revocation List (CRL).
C. On the division's subordinate CA, revoke the certificates it has issued. Publish the Certificate Revocation List. Copy the EDB.LOG file from the subordinate CA to the Certification Distribution Point on your network.
D. On the company's root CA, revoke CA, revoke the certificate of the division's subordinate CA. Publish the Certificate Revocation List (CRL). Copy the CRL file to the Certificate Distribution Point on your network.
E. On the division's subordinate CA, revoke the certificates it has issued. Publish the Certificate Revocation List. Copy the CRL file to the Certificate Distribution Point on your network. Disconnect the CA from the network.

Answer: D
Explanation: By revoking the certificate for the subordinate CA, instead of revoking all of the certificates it has issued, the goal will be achieved with the least amount of administrative effort. Revoking a certificate is a two-

step process first we must revoke the certificate and then create (this is done automatically) and publish the Certificate Revocation List (CRL). Finally, the Certificate Revocation Lists (CRLs) must be accessible to all users. It should be put in a network share and the users should have appropriate (read) permission to the share.

Incorrect Answers:
A: Revoking all certificates that the CA has issued is a daunting administrative task. It is better to revoke the certificate for the CA itself.
B: The Certificate Revocation Lists (CRLs) must be accessible to all users. It should be put in a network share and the users should have appropriate (read) permission to the share.
C: Revoking all certificates that the CA has issued is a daunting administrative task. It is better to revoke the certificate for the CA itself. The edb.log file is not used for revoking certificates.
E: Revoking all certificates that the CA has issued is a daunting administrative task. It is better to revoke the certificate for the CA itself.

QUESTION NO: 76
You are the administrator of TestKing's network. The network consists of two Windows 2000 server computers and 50 Windows 2000 Professional computers. You are using DHCP to automate the assignment of the TCP/IP configurations of the client computers. You configure the DHCP server to automatically update your DNS server's forward and reverse lookup zone files with the DHCP client information.

You discover that 15 of the client computers are referenced by PTR (pointer) records in the reverse lookup zone. There are no PTR records for the remaining 35 client computers.

How should you resolve this problem?

   A.   Configure the client computers so that they register their A (host) records with the DNS server.
   B.   Configure the client computers so that they do not register their domain name with the DNS server.
   C.   Configure the DHCP server to enable updates for client computers that do not support dynamic update
   D.   Configure the DHCP server to always update DNS, even if a client computer does not request it.

Answer: C
Explanation: In this scenario, 35 computers do not get their PTR (pointer) records registered in DNS. All clients computer have their host (A) records registered in DNS. The DHCP server is configured to automatically register both A (Host) records (in forward zone) and PTR (pointer) records (in reverse lookup zone). This not the default setting. Usually Windows 2000 DHCP clients register their own A (host) register in DNS. What might occur in this scenario is that both the DHCP server and the 2000 client try to register the same A (host) record, which may result in missing PTR (Pointer) records. It would be better the change the DHCP setting to change the setting from "always update DNS, even if client computer does not request it" to "enable updates for client computers that do not support dynamic update". By default Windows 2000 clients register each host records directly to the DNS server and request that the DHCP service register the PTR (pointer) record. The

DHCP service adds the PTR (pointer) records to the zone and cleans up the PTR (pointer) and 'A' (Host) records in the zone upon lease expiration. The DHCP service also registers both the 'A' (Host) and PTR (pointer) records for legacy clients, and performs any necessary cleanup action.

Incorrect Answers:
A: The problem is registration of PTR (Pointer) records not A (host) records. By default, Microsoft Windows 2000 clients register their host records directly to the DNS server.
B: The problem is registration of PTR (Pointer) records not A (host) records. Disabling the default behavior of Windows 2000 clients to register their domain name with the DNS server will not help registering the PTR (Pointer records).
D: The DHCP server is already configured to always update DNS even if a client computer does not request it; it updates both the forward and the reverse lookup zones of the clients.

QUESTION NO: 77
You are the administrator of TestKing's network. The network consists of a single Windows 2000 domain and uses TCP/IP exclusively as its transport protocol. You use DHCP assign addresses to your Windows 2000 Professional client computers.

You add 20 new Windows 2000 Professional client computers to your network. Users report that occasionally they cannot access network resources located on servers. However, workgroup resources are sometimes available. The inconsistency in server access does not appear to follow any pattern.

You inspect the TCP/IP configuration of a computer that is experiencing this problem and find that it is using the address 169.254.0.16, which is not a valid address in your network.

What should you do to resolve this problem?

    A.   Configure the client computers to use only DHCP-assigned addresses
    B.   Configure the client computers to only accept addresses from authorized DHCP servers
    C.   Add enough new addresses to the existing DHCP scope to include the new client computers
    D.   Create a new scope on the DHCP server to include the new client computers

Answer: C
Explanation: In this scenario 20 new computers are added. Sometimes network resources are not available to clients. One client with this problem has the private APIPA address 169.254.0.16. This type of address is assigned when the DHCP server are unable to provide IP configuration to the client. The problem is that the DHCP server occasionally runs out of IP addresses. This problem is solved by extending the DHCP scope with new IP addresses.

Incorrect Answers:
A: If the new clients had static IP addresses, they would never be able to access any network resource. They are already DHCP clients, but the DHCP cannot always provide proper IP configuration.

Leading the way in IT testing and certification tools, www.testking.com

B: It seems unlikely that an unauthorized DHCP server would not lease an IP address in the private range of 169.254.xx.xx. The more likely cause of the problem is that the DHCP server occasionally runs out of IP addresses.

D: It is not necessary to create a new scope. It would be better to extend the existing scope.

QUESTION NO: 78
You are the administrator of a Windows 2000 network. The network consists of two Windows 2000 server computers named server1 and server2, and 75 Windows 2000 Professional computers.

Server1 is a DHCP server. The TCP/IP configuration of all the Windows 2000 Professional computers is provided by the server1 DHCP server.

TestKing's technical-support personnel belong to the Helpdesk global group. To allow the technical-support personnel to respond to support calls more effectively, you want them to have only Read access to the DHCP console and the DHCP leases information.

What should you do?

   A.   Place the Helpdesk global group in the DHCP Users group
   B.   Add the members of the Helpdesk global group to the built-in group named Pre-Windows 2000 Compatible Access
   C.   In the DHCP console on the server1 DHCP server, select **Manage authorized servers** and add the Helpdesk global group to the list
   D.   On the server1 DHCP server, grant the Helpdesk global group Read permission on the *Systemroot\system*\system32\DHCP folder

Answer: A
Explanation: The DHCP Users group provides a way to grant read-only console access to the DHCP server. Other users or groups added as members of this group are granted the right to view, but not modify, data for the applicable server in the DHCP console.

Incorrect Answers:
B: Adding the members of the Helpdesk group to the group Pre-Windows 2000 Compatible Access would give access to some parts of the Active Directory. It would give them access to the DHCP information.
C: After selecting manage authorizes servers in the DHCP console a list of servers will be presented. The Helpdesk global group cannot be added to this list.
D: Read access to the DHCP console and to DHCP lease information cannot be set by NTFS file permission. Instead use the DHCP Users built-in group.

QUESTION NO: 79

You are the enterprise administrator for a Windows 2000 Domain that contains Windows 2000 Professional computers. You install Windows 2000 DHCP server on a member server in the domain. The DHCP server is located on the same network segment as the Windows 2000 Professional computers. You create and activate a DHCP scope for the network segment. The Windows 2000 Professional computers are configured as DHCP client computers, but they do not receive IP addresses.

What should you do so that each DHCP client computer receives an IP address?

    A.   In the Device Manager console, start the DHCP service
    B.   Move the DHCP server to the same site as the Windows 2000 Professional computers
    C.   In Active Directory, authorize the DHCP server
    D.   Define a DHCP option Class for the Windows 2000 Professional computers.

Answer: C
Explanation: In an Active Directory environment (Windows 2000 Domain) the DHCP servers must be authorized in the Active Directory before they are allowed to start. This is a precaution which prevents rogue DHCP servers from starting.

Incorrect Answers:
A: We use Device Manager to configure hardware devices not to start services.
B: As the DHCP server is located on the same network segment as the client they already belong to the same site.
D: The DHCP option Class is used to enable different DHCP configuration for different groups of computers in one single scope. Defining an DHCP option Class would not make the DHCP server start working.

QUESTION NO: 80
You are the administrator of TestKing's network. The network consists of three network segments connected by a router as shown in the exhibit. .

Leading the way in IT testing and certification tools, www.testking.com

Subnet 1

Subnet 1 scope
Subnet 2 scope
Subnet 3 scope

DHCP server

Subnet 2

Router
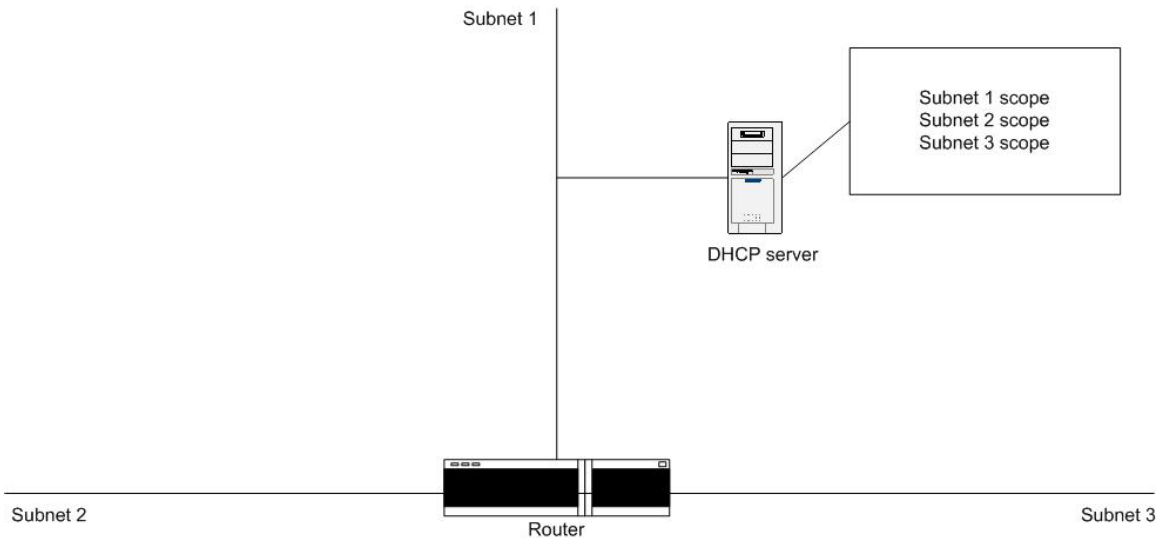
Subnet 3

You install the DHCP server service on a Windows 2000 server computer to automate the configuration of client computers on your network. You create scopes for each subnet's range of addresses and activate each scope.

Users from Subnet 2 and Subnet 3 report that they cannot connect to the network. Users from Subnet 1 report no connectivity problems. You discover that computers on subnets 2 and 3 are not receiving a TCP/IP configuration from the DHCP server.

What should you do to resolve this problem?

    A.   Install the DHCP Relay Agent service on the DHCP server.
    B.   Install the DHCP Relay Agent service on a computer on each remote subnet.
    C.   Install the WINS server service on a Windows 2000 server computer and configure the client computers to use WINS to find the DHCP server.
    D.   Install the WINS proxy Agent service on a computer on each remote subnet.
    E.   Install the DNS server service on a Windows 2000 Server computer and configure the client computers to use DNS to find the DHCP server.
    F.   Install a DNS caching-only server on a computer on each remote subnet.

Answer: B
Explanation: A DHCP server can provide IP addresses to client computers on remote multiple subnets only if the router that separates them can act as a DHCP relay agent. Apparently this router is not BOOTP-enabled, or in other words RFC 1542-compliant and the remote clients are unable to reach the DHCP server. Configure a BOOTP/DHCP relay agent on the remote client subnets. The relay agent can be located on the router itself or on a Windows 2000 Server computer running the DHCP Relay service component. The relay agent should be configured with the IP address of the DHCP server.

Incorrect Answers:

A: The DHCP Relay Agent service must be installed on the remote clients subnets not on the DHCP server itself.
C: The client computers make the initial connection the DHCP server using broadcasts. The DHCP relay agent will pass these broadcasts to the DHCP server. It is not necessary of a WINS server.
D: WINS proxy agents are used for NON-WINS clients like UNIX, OS/2. Windows 2000 is a WINS clients.
E: The clients would not be able to use a DNS server without first getting TCP/IP configuration from the DHCP Server. DHCP helps in finding the DNS server, not the opposite way around.
F: The clients would not be able to use a DNS server without first getting TCP/IP configuration from the DHCP Server.

QUESTION NO: 81
You are the network administrator for Trey Research. Trey Research's network consists of 90 client computers and 50 portable computers, all running Windows 2000 Professional. Only 20 of the users of the portable computers will ever be in the office at the same time. To accommodate the number users on the network, Trey Research purchases a subnetted Class B subnet with a 25-bit mask.

All users need access to the Internet while in the office. How should you configure DHCP?

  A.   Create two scopes that have different lease durations
  B.   Create manual reservations for all portable computer users
  C.   Create one scope that has two user classes, each with a different lease duration
  D.   Create one scope that has two vendor classes, each with a different lease duration.

Answer: C
Explanation: The problem in this scenario is that only 7 bits (32-25) can be used for the host, which only provides for 126 concurrent hosts on the network, but we have 140 computers. Therefore the IP lease duration of the LapTaps should be lowered. In this scenario we must create one user class for the portable computers and one user class for the stationary office computers, each with different lease duration. User classes allows us to differentiate between DHCP clients by specifying a User Class option. When available for client use, this option includes a user-determined class ID that can help to group clients of similar configuration needs within a scope.

Reference:
Microsoft DHCP Vendor and User Classes (Q266675)
How to Create a New DHCP User or Vendor Class (Q240247)

Incorrect Answers:
A: We cannot configure a scope to be used by certain computers without using the user class option.
B: A manual reservation of an IP address would be counterproductive, since those IP addresses couldn't be used by other computers. Lowering the lease time of LapTap's is the correct solution.

D: Vendor classes are most helpful to vendors for managing DHCP option assignments based on vendor-specific needs without disturbing other non-vendor DHCP clients. Vendor classes cannot be used to differentiate between the LapTops and the office computers. User classes have to be used instead.

QUESTION NO: 82
You are the administrator of Windows 2000 network. The network consists of one Windows 2000-based DHCP Server, two routers and 100 Windows 2000 Professional computers. The Windows 2000 Professional computers are distributed over four segments.

The TCP/IP configuration of all the Windows 2000 Professional computers is provided by the DHCP Server. The DHCP Server is in one of the four segments and has scopes that are configured for all four segments.

The routers do not forward the DHCP requests from the Windows 2000 Professional computers.

Each router has three interfaces. You want to enable and configure the DHCP Relay Agent to allow all Windows 2000 Professional computers to receive an IP address from the DHCP Server.

On which interface should you enable and configure the DHCP Relay Agent?

(To answer click the **Select and Place** button, and then drag the box to the appropriate router interfaces. The box may be used more than once)

<div style="border:1px solid black; display:inline-block; padding:4px">

Select And Place

</div>

Interface with DHCP
Relay Agent

35 Windows 2000
Professional Computers

25 Windows 2000
Professional Computers

20 Windows 2000
Professional Computers

Router

Router

20 Windows 2000
Professional Computers

Answer:

Interface with DHCP
Relay Agent

35 Windows 2000
Professional Computers

25 Windows 2000
Professional Computers

20 Windows 2000
Professional Computers

Router

Router

20 Windows 2000
Professional Computers

Explanation: Each router has three interfaces. We much decide on which of these interface we put a DHCP Relay agent. We should put the DHCP Relay agent on the three LAN interfaces which connects to the three segments, not including the segment with the DHCP server, which have Windows 2000 Professional computers. On the leftmost Router we put a DHCP Relay agent on the "west" and the "north" interfaces, but not on the "east" interface which only connects to the 2nd router.
On the rightmost Router we put a DHCP Relay agent only on the "north" interface.
The "west" interface connects only to the 1st router.
The "south" interface connects to the segment with the DHCP Server.

Incorrect Answers:
Do not put the DHCP Relay Agent on the LAN interface which connects to the segment with the DHCP Server. The DHCP server will service this clients.
Do not put the DHCP Relay Agent on LAN interfaces connecting to segments with no client computers. There will be no DHCP client initiated communication from this segment.

QUESTION NO: 83
You are the enterprise administrator of a Windows 2000 Domain. All client computers in the domain are either Windows 98 computers or Windows 2000 computers. Your Windows 2000 users run an Internet application that must access files from a Windows NT computer named WNT_101. None of your Windows 2000 computers can connect to WNT_101, but WNT_101 can connect to every Windows 2000 computer.

What should you do?

A.   Release and renew the IP address of Windows NT_101
B.   Select the **Enable updates for DNS clients that do not support dynamic update** check box
C.   Clear the **Discard forward (name-to-address) lookups when lease expires** check box
D.   Set the DNS zone for the Windows 2000 Domain to **Active Directory Integrated Primary.**

Answer: B
Explanation: A Windows 2000 domain uses Active Directory. Active Directory requires DNS for name resolution. Windows 2000 clients are able to communicate with each other. They use Dynamic DNS (DDNS) to register themselves in the DNS zone of the domain. Windows NT 4.0 computers are not able to register themselves in DNS. This is the reason the no one can connect to the WNT_101 machine. By configuring the DHCP server to **Enable updates for DNS clients that do not support dynamic update** the DHCP server will register A (host) and PTR (pointer) records in DNS for WNT_101. The computer would then be accessible on network.

Incorrect Answers:
A: The NT_101 computer is able to connect to the Windows 2000 computers. There is nothing wrong with the IP configuration of NT_101.

Leading the way in IT testing and certification tools, www.testking.com

C: By clearing the **Discard forward (name-to-address) lookups when lease expires** check box on the DHCP server, the DHCP server will not remove A (Host) records when leases expire. This is not a solution to the problem at hand.

D: Changing the zone to an Active Directory Integrated zone will not enable the NT_101 computer to be registered in the DNS zone.

QUESTION NO: 84

You are the administrator of Windows 2000 network. The network consists of 10 segments. These segments are connected by four Windows 2000 server-based routers named Router1, Router2, Router3 and Router4. Routing and remote access is enabled as a router on these four servers. To exchange routing information, the four servers use RIP version 2 for IP.

There are two other routers on the network that use RIP version 2 to exchange routing information. These other routers might have been erroneously configured and, consequently, contain incorrect routing information.

You want to ensure that Router1, Router2, Router3 and Router4 do not process routes received from any other router than Router1, Router2, Router3 and Router4.

How can you configure the four routers to accomplish this goal? (Choose all that apply)

A. Configure the RIP routing protocol on the four routers to RIP peer filters. List the other three routers as RIP peers.

B. Configure each RIP interface on the four routers to unicast announcements to RIP neighbors. List the other three routers as RIP neighbors.

C. Configure each RIP interface on the four routers to use password authentication. Use the same password on all four routers.

D. On each RIP interface on the four routers, configure routes for outgoing routes. Announce only routes in the route ranges of the network IDs that are connected to the four routers.

Answer: A, B, C, D
Explanation:
A: We can configure each RIP router with a list of routers (by IP address) from which RIP announcements are accepted. By default, RIP announcements from all sources are accepted. By configuring a list of RIP peers, RIP announcements from unauthorized RIP routers are discarded.
B: By default, RIP either broadcasts (RIP version 1 or RIP version 2) or multicasts (RIP v2 only) announcements. To prevent RIP traffic from being received by any node except neighboring RIP routers, the Windows 2000 router can unicast RIP announcements to neighboring RIP routers.
C: To prevent the corruption of RIP routes by an unauthorized RIP router in a RIP version 2 environment, you can configure RIP v2 router interfaces to use simple password authentication. Received RIP announcements that do not match the configured password are discarded.

D: We can configure route filters on each RIP interface so that the only routes considered for addition to the routing table are those that reflect reachable network IDs within the internetwork Neighbors.

QUESTION NO: 85
You are the administrator of TestKing's WAN. The network consists of 10 internal subnets in two physical sides connected by routes as shown in the exhibit. .
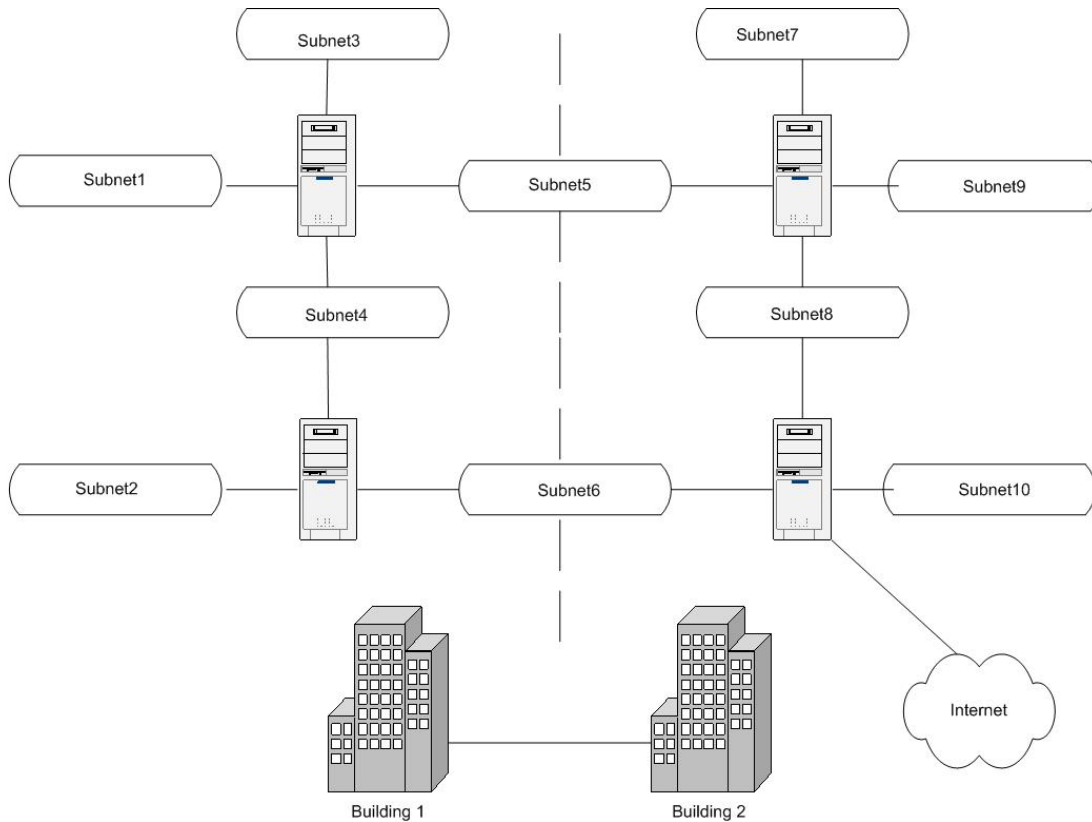
You have an additional subnet that is configured for access to the Internet. The routers on the network will be multihomed Windows 2000 server computers running routing and remote access.

You want to accomplish the following goals.

- **Administrative overhead for configuration of routing tables on each router will be minimized.**
- **Broadcast traffic for configuration of routing tables on each router will be minimized.**
- **In the event of a router failure, link redundancy within 10 minutes will be ensured.**
- **Convergence time of less than one minute for all known routers on all routers will be ensued.**
- **Internal routing information will never be exposed to external router.**

You take the following actions:

- **Install RIP version 1.**
- **Configure RIP to use all interface on all multihomed computers.**
- **Enable RIP authentication by specifying a password on each interface.**

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

    A.   Administrative overheads for configuration of routing tables on each router is minimized.
    B.   Broadcast traffic for configuration of routing tables on each router is minimized.
    C.   In the event of a router failure, link redundancy within 10 minutes is ensured.
    D.   Convergence time of less than one minute for all known routes on all routers will be ensued.
    E.   Internal routing information is never exposed to external routers.

Answer: A
Explanation: RIP V1 facilitates the automatic exchange of routing information.

Incorrect Answers:
B: Broadcast traffic for routing table configuration is not minimized because all RIP V1 route announcements are addressed to the IP Subnet and MAC-Level, even non-RIP hosts receive RIP announcements. RIP broadcasts every 30 seconds. The amount of broadcasts traffic can become significant on large networks.
C: By default each router table entry learned through RIP is given a timeout of 3 minutes past the time it was received in a RIP announcement from a neighboring RIP router. There is at least a distance of four hops between routers in the exhibit, so the convergence time is greater than 10 minutes.
D: Since neighboring routers could need up to 3 minutes a convergence time of less than 1 minute is impossible.
E: RIP authentication by password has been specified on each interface, but RIP V1 does not support password authentication. Only RIP V2 supports password authentication.

QUESTION NO: 86
You are the administrator of a Windows 2000 network. The network consists of two segments connected by a router. Each segment contains two Windows 2000 server computers and 50 Windows 2000 Professional computers.

The network has one DHCP server that has active scope for both segments. The IP addresses configured in the two scopes are 10.65.1.0/24 for one segment and 10.65.2.0/24 for the other segment. The IP address for the DHCP server is 10.65.1.2.
The network is shown in the exhibit.

Leading the way in IT testing and certification tools, www.testking.com

50 Windows 2000
Professional Computers

50 Windows 2000
Professional Computers

10.65.1.2

Router

Windows 2000
server computer

Windows 2000
server computer
Server Type: DHCP
Scope: 10.65.1.0/24
Scope: 10.65.2.0/24

Windows 2000
Server Computer

Windows 2000
Server Computer
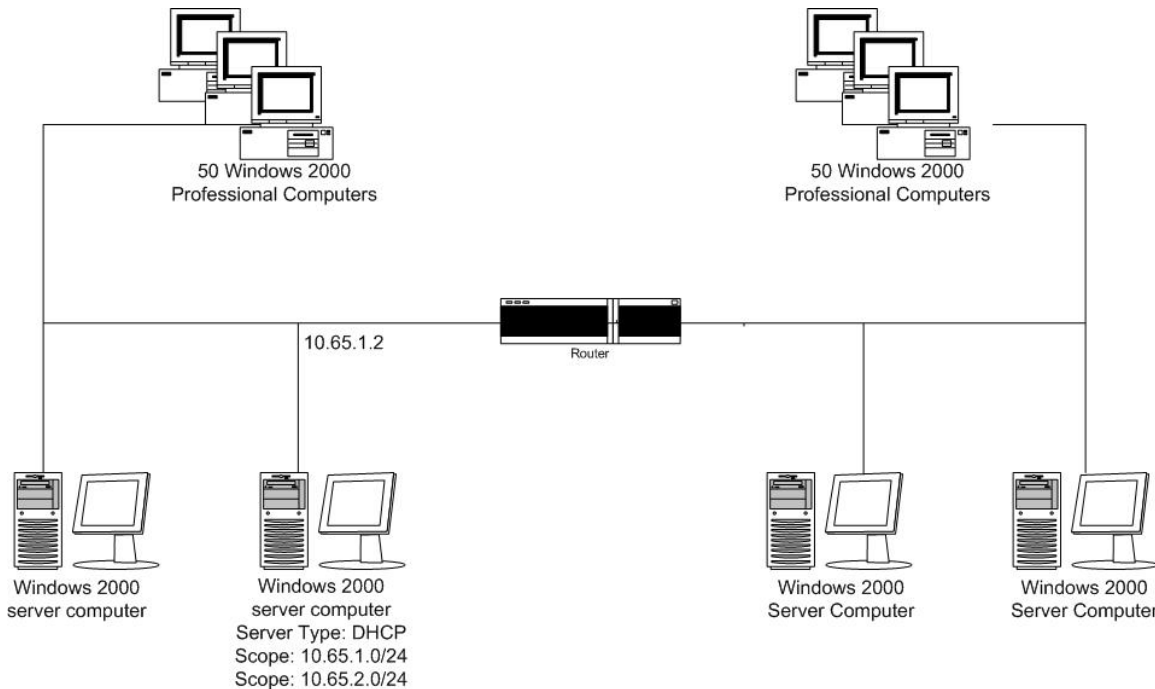
Users in the segment that does not have the DHCP server report that their 2000 Professional computer are using IP addresses in the range of 169.254.0.0/16. Windows 2000 Professional computers in the other segments use the IP addresses in the range of 10.65.1.0/24.

You want Windows 2000 Professional computers in the segment that does not have DHCP server to automatically use the IP addresses in the range of 10.65.2.0/24.
How should you configure the network to accomplish the goal?

    A.   Enable and configure DHCP relay agent service on the DHCP server.
    B.   Enable and configure DHCP relay agent server on a server in the segment that does not have the DHCP server.
    C.   On the DHCP server, configure a packet filter to receive IP packets that use the BOOTP port.
    D.   On the server in the segment that does not have a DHCP server, configure a packet filter to receive IP packets that use the BOOTP port.

Answer: B
Explanation: Users in the remote segment received IP addresses of 169.254.0.0/16, private APIPA addresses, which are assigned when a DHCP server cannot be reached. A DHCP server can provide IP addresses to client computers on remote multiple subnets only if the router that separates them can act as a DHCP relay agent. Apparently this router is not BOOTP-enabled, or in other words RFC 1542-compliant and the remote clients are unable to reach the DHCP server. Configure the BOOTP/DHCP relay agent on the remote client subnets. The relay agent can be located on the router itself or on a Windows 2000 Server computer running the DHCP Relay service component. The relay agent should be configured with the IP address of the DHCP server.

Incorrect Answers:

A: The DHCP Relay agent server should be configured on the remote segment not on the DHCP server.
C: It is the router that blocks the DHCPINFORM messages. Changing packet filters on the DHCP will not help.
D: It is the router that blocks the DHCPINFORM messages. A packet filter on the remote segment would not enable communication with the remote clients.

QUESTION NO: 87
You are the administrator of a Windows 2000 domain. The domain has a Windows 2000 member server computer named Houston. Routing and remote access is enabled for remote access on Houston. The domain also has a DHCP server. The domain is in native mode.

Users in the domain dial in the network by using Windows 2000 Professional portable computers. The configuration of the dial-up connection on the Windows 2000 Professional computer is set to obtain an IP address automatically. You do not want to change this configuration.

For administrative purposes, you want to designate a fixed IP address for each of the users. All users should receive a different fixed IP address when a dial-up connection is made.

How should you configure the network to accomplish this goal?

A. On the Houston Remote Access service, create a static address pool so that it has only the IP address of the remote access dial-in interface. Use a mask of 0.0.0.0.
B. On the Houston remote access service, create a static address pool for IP address assignment. Use a mask of 255.255.255.255.
C. On the DHCP server, create a reservation that uses a specific IP address for each user.
D. In the active directory user and computers console, assign static IP address for each user.

Answer: D
Explanation: A static IP addresses for each individual user is set in the Active Directory Users and Computers console by selecting Users, right-clicking appropriate User, select Properties, choose Dial-in tab, and then enable Static IP address and provide it.

Incorrect Answers:
A: A static address pool is used to dynamically give remote users IP configuration information. The remote users will not receive a designated fixed IP address.
B: A static address pool will not provide designated fixed IP address assignments.
C: Creating a reservation for each individual user is possible, but would be an administrative nightmare.

QUESTION NO: 88

Leading the way in IT testing and certification tools, www.testking.com

You are the administrator of Windows 2000 domain. The domain has a Windows 2000 member server computer named Vegas. Routing and remote access is enabled for remote access on Vegas. Some of the remote access client computers require the use of CHAP.

You enable CHAP on Vegas. You also configure the appropriate remote access policy to use CHAP. However, users who require CHAP report that they are not able to dial in to Vegas.

What should you do?

    A.   Configure Vegas to prohibit the use LAN manager authentication.
    B.   Configure Vegas to disable use of link control protocol (LCP) extensions.
    C.   Configure the user accounts by selecting **Store passwords using reversible encryption**. Set the user passwords to change the next time each user logs on.
    D.   Configure the user account to use static IP address when they dial into the network.

Answer: C
Explanation: To enable CHAP-based authentication, we must enable CHAP as an authentication protocol on the remote access server, enable CHAP on the appropriate remote access policy, enable storage of a reversibly encrypted form of the user's password, force a reset of the user's password so that the new password is in a reversibly encrypted form, and enable CHAP on the remote access client running Windows 2000. When we enable passwords to be stored in a reversibly encrypted form, the current passwords are not in a reversibly encrypted form and are not automatically changed. We must therefore either reset user passwords or set user passwords to be changed the next time each user logs on

Incorrect Answers:
A: LAN manager authentication is used for legacy clients, for example DOS, but is of no use here.
B: Disabling LCP extensions would help in troubleshooting certain Internet Service Provider Login problems. It would not help with this RRAS dial-in problem.
D: This is an authentication problem, not an IP configuration problem.

QUESTION NO: 89
You are the administrator of a Windows 2000 domain. The Domain has a Windows 2000 member server computer named Helsinki. Routing and remote access is enabled for remote access on Helsinki.

Users in the domain are able to dial in to the network by using their Windows 2000 Professional computers.

Your company has a group named sales. You want to allow members of the sales group to use a smart card for the remote authentication. The dial-in permission for all users in the sales group is set to control access through remote access policy.

You create a new access policy named sales access. This remote access policy grants remote access to members of the sales group any time of the day. This remote access policy is the first policy on the list of remote access policies on Helsinki.

Members of the sales group are able to dial in to the network, but they report that they are unable to use a smart card for remote authentication. You want to ensure that members of the sales group are able to use the smart card authentication method.

What should you do?

    A.   In active directory, add Helsinki to the Pre-Windows 2000 compatible access group.
    B.   Enable EAP as an authentication method on the Helsinki remote access server and the Windows 2000 remote access client computers. Enable EAP in the profiles of the sales access remote access policy.
    C.   For all the member of the sales group, select **stored passwords using reversible encryption**.
    D.   For all the members of the sales group, configure the user account to be trusted for delegation.

Answer: B
Explanation: Smart Card Authentication requires the use of the Extensible Authentication Protocol (EAP). EAP has to be configured at the RAS server, at the RAS clients, and in profiles o the remote access policy.

Incorrect Answers:
A: The Pre-Windows 2000 Compatible Access is a backward compatibility group which allows read access on all users and groups in the domain. Adding Helsinki to it would not enable smart card authentication.
C: The stored passwords using reversible encryption setting is used when the CHAP protocol is enabled. It is not used to enable smart card authentication.
D: The trusted for delegation privilege enables the user (or computer) to access resources on another computer. It is not used to enable smart card authentication.

QUESTION NO: 90
You are the administrator of TestKing's network. The network consists of one Windows 2000 domain running in native mode. You are not running Certificate Services in the domain.

Your company is a sales organization and has 150 salespeople. When these salespeople are out of office, they require file and print services, e-mail and access to the company's product and inventory database. These salespeople belong to a group named SalesMobile.

Your company has dedicated T1 access to the Internet. Your company also uses a virtual private network (VPN) to reduce the costs and hardware required to support the salespeople.

You want to accomplish the following goals:

- **Required network resources will be accessible to all salespeople.**
- **Connections to the network will be made only by salespeople.**
- **Sensitive company data will be kept confidential over the VPN connections.**
- **Access to the network will only take place during business hours.**
- **All salespeople will be able to connect to the network simultaneously.**

You take the following actions:

- **Install routing and remote access on a Windows 2000 server computer and configure virtual private networking.**
- **Grant the salespeople the Allow Access dial-in permission.**
- **Edit the default remote access policy to grant remote access permission.**
- **Edit the default remote access profile to require strong encryption of data.**

Which result or results do these actions produce?

    A.   Required network resources are accessible to all salespeople.
    B.   Connections to the network are made only by salespeople.
    C.   Sensitive company data is kept confidential over the VPN connections.
    D.   Access to the network only takes place during business hours.
    E.   All salespeople are able to connect to the network simultaneously.

Answer: A, C
Explanation:
A: Salespeople have access to the network resources, since they have the Allow Access dial-in permission. The default remote access profile will also allow access, since it has no conditions.
C: The default remote access profile (RAP) is set to require strong data encryption. There is no other way to get access, so all company data are kept confidential.

Incorrect Answers:
B: The default dial-in permission in native mode is Control Access through Remote Access Policy. This applies to all user accounts in the domain, except the Salespeople users who have Allow access. The default remote access policy has no restrictions so every user would be able to get remote access.
D: No time restriction policy has been selected in default RAP. The default setting is to allow dial during all times. Access will not be restricted to business hours.
E: Only 10 PPTP ports are configured by default. The 150 sales people would not be able to connect simultaneously with only 10 ports. The PPTP ports setting must be increased to at least 150.

QUESTION NO: 91
You are the administrator of TestKing's network. You are configuring a Windows 2000 network for dial up access. Your users need to access their computers from home. To increase security your company issue smart cards to all users who have dial up access.

Leading the way in IT testing and certification tools, www.testking.com

You need to configure your Routing and Remote Access server. What should you do? (Choose two)

A.   Select the **Extensible Authentication Protocol (EAP)** check box.
B.   Select the **Microsoft encrypted authentication version 2 (MS-CHAP v2)** to check box.
C.   Install a computer certificate on the routing and remote access server.
D.   Install a smart card logon certificate on the routing and remote access server.
E.   Install a computer certificate on the dial-up access client computer.

Answer: A, D
Explanation: The Extensible Authentication Protocol (EAP) is required for authentication using smart cards. A smart card logon certificate must be installed on routing and remote access server.

Incorrect Answers:
B: EAP, not MS-CHAP V2, must be used for smart card user authentication.
C: A smart card logon certificate, not a computer certificate, must be installed.
E: A smart card logon certificate, not a computer certificate, must be installed.

QUESTION NO: 92
You are the administrator of TestKing's network. Your company employs account executives who need access to the latest company data when they are traveling. You want to ensure that your company will establish the network connection for your account executives regardless of where the call originates.

Your company also allows vendors access to the network by routing and remote access to submit purchase orders. To ensure network security, your company wants to specify the location from which vendors can connect.

You want to configure TestKing's routing and remote access server to facilitate access for account executive and vendors. Which three actions should you take to ensure this configuration? (Choose three)

A.   Set the **Callback** option to **Always Callback to** for the account executives.
B.   Set the **Callback** option to **Set by Caller** for the account executives.
C.   Set the **Callback** option to **No callback** for the vendors.
D.   Set the **Callback** option to **Always Callback to** for the vendors.
E.   Set the **Callback** option to **Set By Caller** for the vendors.
F.   Enable link Control protocol (LCP) extensions.
G.   Enable EAP.

Answer: B, D, F
Explanation: By configuring the Callback option to Set by Caller for the account executives, the executives will be able to dial-in regardless where the call originates.

By configuring the Callback option to Always Callback to for the vendors, the company can specify from where the vendors are allowed to dial-in.

Enabling link Control protocol (LCP) extensions will enable callback during the LCP negotiation of LCP. And callback is used in the Callback option in this scenario.

Incorrect Answers:
A: The account executives must be able to call in regardless of location. The Callback option must be set to Set By caller, not Always callback to.
C: The No Callback option would allow the vendor to call in regardless of location, which shouldn't be allowed.
E: The vendors must not be able to call in regardless of location. The Callback option must be set to Always callback to, not Set By caller.
G: EAP would require further configuration to work.

QUESTION NO: 93
You are the administrator of TestKing's network, which consists of a single Windows 2000 Domain. The relevant portion of its configured is shown in the exhibit. .
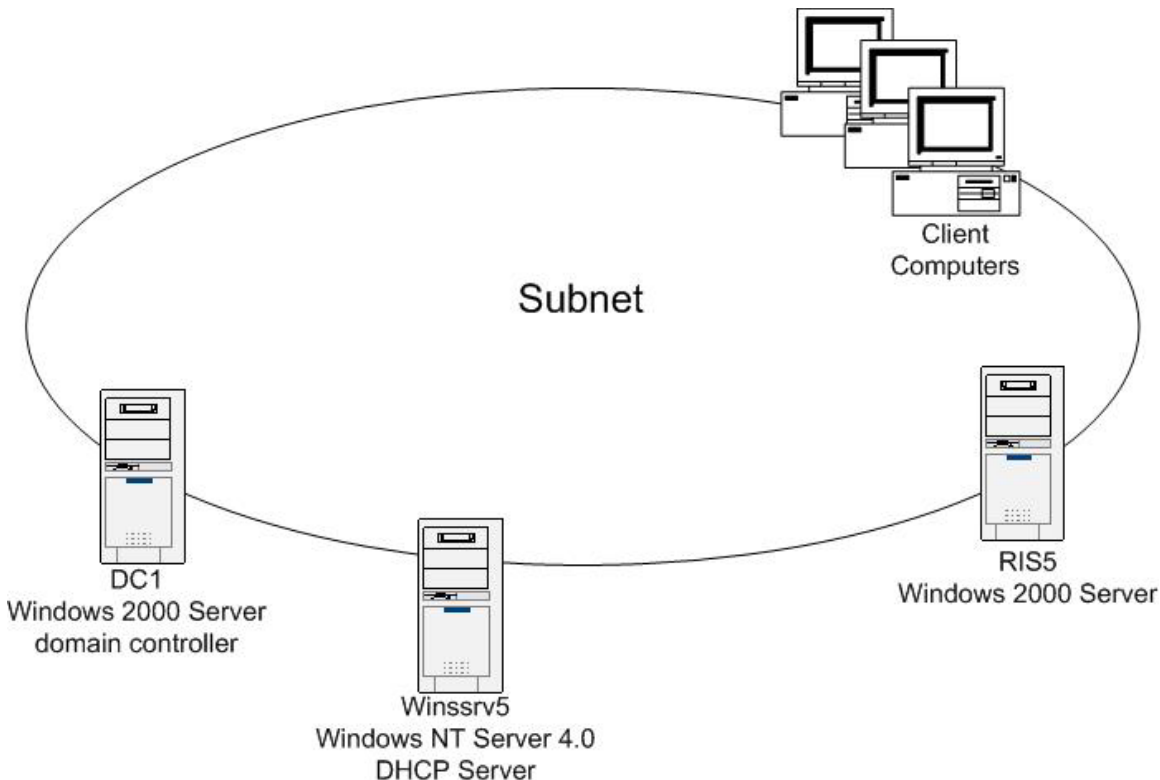
RIS5 will be used to deploy Windows 2000 Professional to new client computers. You add RIS5 to the domain and install RIS on it. You configure RIS5 to obtain IP addressing information from Winsvr5.

Leading the way in IT testing and certification tools, www.testking.com

You try to use RIS to deploy Windows 2000 Professional to a PXE-compliant client computer. However, this computer cannot connect to RIS5. When you examine the event log on RIS5, you discover the following error message: "BINL will not respond to client requests."

How should you correct this problem?

A. Use the Active Directory sites and services console to authorize RIS5 as a DHCP server in the domain.
B. Use the Active Directory sites and services console to authorize Winsvr5 as a DHCP server in the domain
C. Create a DHCP reservation for RIS5 on winsvr5
D. Create DHCP reservations for new client computers on Winsvr5.

Answer: B
Explanation: In this scenario the Boot Information Negotiation Layer (BINL) service must be authorized even though DHCP may not be running on the server and non-Windows 2000 DHCP servers are being used. If our network environment includes other non-Windows 2000 DHCP servers, they must be authorized. Authorizing a server sets an attribute in the Active Directory that allows it to function. In our scenario the DHCP server on the Windows NT machine Winsrv5 has to be authorized in the Active Directory.

Incorrect Answers:
A: RIS5 is not a DHCP server. Winsrv5 not RIS5 has to be authorized in Active Directory.
C: Creating a reservation for the RIS server will not solve the problem. The DHCP server is not allowed to start. It has to be authorized.
D: Creating reservations will not solve the problems. The DHCP server is not allowed to start. It has to be authorized.

QUESTION NO: 94
You are the administrator of TestKing's network, which consists of a single Windows 2000 Domain. Your human resources department maintains a confidential database server named HRSvr1. because the information in the database is essential to TestKing's successful operation, HRSvr1 requires he highest possible level of security.

The only server that exchanges confidential information with HRSvr1 is a middle-tier application server named HRClt2 provides client query responses to HR users. These responses are secured by application-level encryption.

A former administrator configured custom IPSec policies on both HRSvr1 and HRClt2. however, you suspect that these policies do not provide an adequate level of security for traffic between the two servers. When you run the IP security monitor on HRClt2, you receive the output shown in the exhibit.

Leading the way in IT testing and certification tools, www.testking.com

IP Security Monitor

Security Associations:

Policy Name	Security	Filter Name	Source Address	Dest. Address	Protocol	Src. Po	Dest.
Secure Initiat	None	<UnInitializ..	200.1.1.2	200.1.1.3	0	0	

Options...

Minimize

IPSEC Statistics

Active Associations	1
Confidential Bytes Sent	0
Confidential Bytes Received	0
Authenticated Bytes Sent	33,118
Authenticated Bytes Received	71,845
Bad SPI Packets	0
Packets Not Decrypted	0
Packets Not Authenticated	0
Key Additions	0

ISAKMP/Oakley Statistics

Oakley Main Modes	0
Oakley Quick Modes	0
Soft Associations	0
Authentication Failures	0

IP Security is enabled on this computer.

You need to modify the existing IPSec policies to secure all traffic between the two servers. Which two actions should you perform? (Each correct answer presents part of the solution. Choose Two)

    A.   Configure the IPSec policy properties on both servers to include both 2DES and DES algorithms.

    B.   Configure IPSec policy properties on both servers to include both HMAC-SHA and HMAC-MD5 algorithms.

    C.   Configure IPSec session Key PFS (Perfect Forward secrecy) on HRSvr1

    D.   Configure IPSec Master Key PFS (Perfect Forward secrecy) on HRClt2

    E.   Set the IP filter on HRClt2 to include only the IP address of HRSvr1

    F.   Set the IP filter action on both servers to negotiate both authentication header (AH) and encapsulating security payload (ESP) protocol traffic with peer.

Answer: B, C
Explanation:
B: The HMAC-SHA and HMAC-MD5 encryption algorithms are the most secure.
C: Session Key Perfect Forward Secrecy will create a new master key during every session rekey operation. It should be configured on a server that is a part of the domain.

Incorrect Answers:

A: HMAC-SHA and HMAC-MD5 are more secure than DES and 3DES. There is no encryption algoritm called 2DES.
D: IPSec Keys should be configured on servers that are part of the domain (HRSrv1) not on application servers (HRClt2).
E, F: IP filters cannot be used to configure IPSec policies.

QUESTION NO: 95
You administer the network segment used by TestKing's sales department. This department employs 50 salespeople, who use portable computers. Each business day, a maximum of 25 salespeople work on-site. The remaining salespeople work remotely.

Your network segment includes one DHCP server running Windows 2000 server. All the portable computers are DHCP clients. The DHCP server is configured with the characteristics shown in the following table.

IP address range	Lease duration	Conflict detection attempts	Enable dynamic update of DNS records?
172.30.20.51 to 172.30.20.101	3 days	0	Yes

Your department hires 20 new salespeople and issues portable computers to them. The new salespeople will work on-site for several months, and then begin working remotely. However, none of these new users can connect to the network. They receive an error message indicating that their computers cannot obtain IP addresses.

You need to enable the new salespeople to connect to the network. Your solution must prevent the connect problem from happening again. Your solution must also avoid disrupting network communications for existing network users and minimize network traffic associated with DHCP.

What should you do?

A. Delete the existing IP address leases from the DHCP server. Increase the setting for conflict detection attempts to 3. Decrease the lease duration to eight hours.
B. Decrease the lease duration to one day. Increase the setting for conflict detection attempts to 2.
C. On the new salespeople's computers, run the **ipconfig/release** command and then the **ipconfig/renew** command.
D. Disable dynamic update of DNS records. Decrease the lease duration to eight hours. Run the **ipconfig/renew** command on the new salespeople's computers.

Answer: B

Explanation: There are too few IP addresses in this scenario. Either more IP addresses must be added to the scope or IP lease time must be decreased. Decreasing the lease time to one day would release IP addresses when workers take their laptops and work on the field.

By increasing the conflict detection attempts from the default 0 to 2, the DHCP server will determine whether an IP address is already in use on the network before leasing or using the address.

Incorrect Answers:
A: If DHCP server-side conflict detection is used, you should set the number of conflict detection attempts made by the server to use one or two pings at most, not 3. It is unnecessary to delete the IP leases when server-side conflict detection is used.
C: IPconfig/release followed by IPConfig/Renew might solve the short term problem, but the problem would reappear later. This is no long term solution.
D: Decreasing the lease time to 1 day would be better than to decrease it to 8 hours. During one work day the lease might have to be renewed, which increases DHCP traffic. Increasing conflict detection attempts would be a better long term solution then to run the ipconfig/renew command once.

QUESTION NO: 96
You administer the Tailspin Toys network, which consists of a single Windows 2000 Domain. To reduce broadcast traffic in your network, you disable NetBIOS over TCP/IP support on all computers.

The network contains a Windows 2000 Server computer named tswebsrv.tailspintoys.com, which hosts your internal Web site. For this server, you create a CNAME (canonical name) record named IWEB in your DNS zone.

Using your own Windows 2000 Professional computer, you try to access a file share named dropbox on tswebsrv.tailspintoys.com by mapping a drive to \\iweb.tailspintpys.com\dropbox. However, you receive the following error message.
The mapped network drive could not be created because the following error has occurred:
A duplicate name exists on the network.

You establish that no other computer on the network is named IWEB. However, the error persists, and you still require access to dropbox.
What should you do?

    A.   Create a Hosts file on your computer and add an entry for IWEB
    B.   Enable NetBIOS over TCP/IP support on your computer
    C.   Enable NetBIOS over TCP/IP support on tswebsrv.tailspintoys.com
    D.   Use the primary computer name \\tswebsrv to connect to tswebsrv.tailspintoys.com
    E.   Use only the alias \\iweb to connect to tswebsrv.tailspintoys.com

Answer: D

Explanation: The problem in this scenario can occur when we try to connect to the server by using a CNAME alias created in the DNS zone. The server is not "listening" on the alias, and because of this, it is not accepting connections to that name. The solution is to use the primary computer name to connect instead of the alias. In this scenario the primary computer name is \\tswebsrv.

Incorrect Answers:
A: One A (Host) record for IWEB already exists in the DNS zone. Preloading another A (Host) record for IWEB using a Hosts file would make no difference.
B: This is not a NetBIOS name problem, this is a DNS problem.
C: This is not a NetBIOS name problem, this is a DNS problem.
E: The primary name, not the alias name must be used.

QUESTION NO: 97
You are the network administrator for Lucerne Publishing. Your network consists of a single Windows 2000 Domain.

Lucerne Publishing employs a full-time staff. It also contracts authors for short-term projects. All full-time employees use portable computers that run Windows 2000 Professional. These users require remote access to network resource, such as applications and printers. Contracted authors use their personal computers, which run a variety of operating systems, including Windows 98, Windows NT 4.0, and Windows 2000 Professional. The authors require remote access to the network so they can upload draft and revisions to a file share located on a Windows 2000 Server named Srv1.

To ensure connection security, you allow access to the network only by means of a virtual private network (VPN) connection through the Internet. You use PPTP as the VPN protocol, and you configure four VPN servers as a Network Load Balancing (NLB) cluster.

Several authors now report that they experience rejected connections when they log on and try to access srv1. Full-time employees report no problems.
How should you correct this problem?

   A.   Remove the cluster IP address from the server interfaces that receive the PPTP connections
   B.   Remove the dedicated IP address from the server interfaces that receive the PPTP connections
   C.   Edit the default remote access profile to grant access only to VPN connection and to increase the **Disconnect if idle** setting to 10 minutes.
   D.   Edit the default remote access policy to grant access only to NAS Port Type VPN and to increase the **Disconnect If Idle** setting to 10 minutes.

Answer: B
Explanation: If we are using Network Load Balancing to load balance Point-to-Point Tunneling Protocol (PPTP), clients running Windows 95, Windows 98, or Windows NT 4.0 may, under certain circumstances, be unable to connect to a Network Load Balancing cluster.
This problem can occur if the Network Load Balancing hosts use a dedicated IP address on the network adapter to which Network Load Balancing is bound. To avoid the problem, we must remove the dedicated IP address from all Network Load Balancing cluster hosts. This problem does not occur with Windows 2000 clients.

Incorrect Answers:
A: The dedicated IP address, not the cluster IP address, should be removed the server interfaces that receive the PPTP connections.
C: The connections for the downlevel clients are immediately rejected. They are not disconnected because of the **Disconnect if idle** setting. The **Disconnect if idle** is disabled by default.
D: The **Disconnect if idle** is disabled by default. The problem cannot be fixed by restricting access to only to NAS Port Type VPN.

QUESTION NO: 98
You are the administrator for Miller Textiles. The network consists of one Windows 2000 domain named millertextiles.local. For security reasons, you want to ensure that internal name resolution traffic never passes outside the network. You also want to ensure that external name requests are handled by an external DNS server.
What should you do to accomplish these goals?

   A.   Create a new standard primary zone for your local namespace and enter only internal addresses into the host table.
   B.   Create a new Active Directory integrated zone for your logical namespace and enter only internal addresses into the host table.
   C.   Delete the root zone for your local namespace and configure all internal DNS servers to forward name resolution requests to the external DNS server.
   D.   Create a new root zone for the Internet and configure all internal DNS servers to forward all requests to this zone.

Answer: C
Explanation: By deleting the root zone and configure all internal DNS servers to forward name resolutions requests to the external DNS server all external name requests are handled by an external DNS server. The default root zone might contain records to Internet root servers, but that zone is deleted. Also internal name resolution would never be passed to the external DNS server.

Incorrect Answers:
A: An external DNS server must be used for external name resolution.

B: An external DNS server must be used for external name resolution.
D: It's less administrative effort to directly use an external DNS server compared to create on new root zone for the Internet.

QUESTION NO: 99
You are the administrator of a Windows 2000 network. The network has 300 Windows 2000 Professional computers, one Windows 2000-based WINS server, and four Windows 2000 DHCP servers, and eight other Windows 2000 server computers. The 300 Windows 2000 Professional computers and the servers are divided over four different locations named North Building, East Building, South Building and West Building. The WINS server is in the East Building location. The TCP/IP configuration of the WINS client computers is provided by four DHCP servers on the network.

The Windows 2000 Professional computers NetBIOS-based resources in the network.

Because of a malfunction on the WINS server's hard disk, you replace it and restore the WINS database from a backup that is one week old.

After the new WINS server is in place, users report that they cannot browse any of the resources in the other locations.

What should you do to enable users to browse resources in other locations again?

A.   On the WINS server, use Jetpack.exe utility on the WINS database.
B.   On the WINS server, use **Verify Database Consistency** command.
C.   On the Windows 2000 Server computer, use the **Nbtstat -RR** to release and refresh the WINS registrations.
D.   On the WINS client computers, use the **ipconfig/registerdns** command to register names and IP addresses.

Answer: C
Explanation: The command nbtstat –RR releases names registered with a WINS server and then renews their registrations. This will release obsolete records and all WINS clients will get registered properly again.

Incorrect Answers:
A: Jetpack.exe is used for DHCP databases not for the WINS database.
B: Consistency checking helps maintain database integrity among WINS servers that are configured as replication partners. It is not used to fix the records of a single WINS database.
D: IPConfig /RegisterDNS register a host record in a DNS zone, not a NetBios record in the WINS database.

Leading the way in IT testing and certification tools, www.testking.com

QUESTION NO: 100
You are the administrator of TestKing's network. The network consists of 10 Windows 2000 server computers, 200 Windows 2000 Professional computers, and 20 UNIX servers. You are using Windows 2000 as your DNS server. Your DNS zone is considered as an active directory integrated zone. Your DNS zone is also configured to allow dynamic updates.

User report that although they can access the Windows 2000 computers by host name, they cannot access the UNIX servers by host names. What should you do to correct this problem?

    A.   Manually enter A (host) records for the UNIX servers to the zone database.
    B.   Manually add the UNIX servers to the Windows 2000 domain.
    C.   On the DNS server, manually create the Hosts file that contains the records for the UNIX servers.
    D.   Configure a UNIX computer to be a DNS server in a secondary zone.

Answer: A
Explanation: By default Windows 2000 clients can register both A and PTR Records dynamically. The UNIX servers are unable to do it. A (Host) records must be added manually to the DNS zone for these UNIX servers.

Incorrect Answers:
B: The UNIX does not have to join the domain; users just want to access them.
C: A Host file that contains the records for the UNIX servers must be copied to all clients computers, it cannot only be saved at the DNS server.
D: The UNIX computers must be registered in the DNS zone. A UNIX server in a secondary zone will not help.

QUESTION NO: 101
You are the administrator of the contoso.com domain. Your network consists of 7,000 client computers distributed evenly across five sites. Each site has its own Windows 2000 domain, and each site has been delegated authority from your root DNS server to manage its own namespace.

In the site named boston.contoso.com, the local administrator has recently upgraded the two DNS servers that service the subdomain. You suspect that the upgrade to the DNS server has resulted into an incorrect configuration of your zone delegation.
What should you do to verify that your zone delegations are properly reconfigured?

    A.   Start system monitor. Confirm that the counters for DNS; Recursive Query Failures are zero.
    B.   Start system monitor. Confirm that the counters for DNS: Zone Transfer Failures are zero.
    C.   Run the **nslookup -querytype=ns boston.contoso.com.** command with the server options to query the boston.contoso.com server. Ping the records displayed in the output of the **nslookup** command.
    D.   Run the **nslookup –ls- d. boston.contoso.com.** command with the server option set to query the boston.contoso.com server . Ping the records displayed in the output of the **nslookup** command.

Answer: C
Explanation: The nslookup utility is used to verify zone delegation. We can use it to find the NS (=name server, dns server) records. You do this with the command:
nslookup querytyp=ns address.
Then ping the addresses of these records.

Reference: Windows 2000 Server documentation, To verify a zone delegation using the nslookup command

Incorrect Answers:
A: System monitor monitors system performance; it cannot be used to monitor this type of traffic.
B: System monitor monitors system performance; it cannot be used to monitor this type of traffic
D: The nslookup command ls -d boston.contoso.com would give a full listing of the records in that domain.

QUESTION NO: 102
You are the administrator of TestKing's network. Your company has a main office, two branch offices, and two small branch offices. The company's network consists of one Windows 2000 domain. The main office and the two large branch offices are connected by a dedicated T1 lines, as shown in the exhibit. .

The two small branch offices use 128-Kbps ISDN lines and routing and remote access over the Internet to connect to the company's internal network.

You are designing your DNS name resolution environment. You want to accomplish the following goals:

- **DNS name resolution traffic across the WAN links will be minimized.**
- **DNS replication traffic across the WAN links will be minimized.**
- **DNS replication traffic across the public WAN links will be secured.**
- **Name resolution performance for the client computers will be optimized.**

You take the following actions:

- **Install the DNS server service on one server at each office.**
- **Create the standard primary zone at the main office.**
- **Create a standard secondary zone at the four other offices.**
- **Configure client computers to query their local DNS server.**

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

A.   DNS name resolution traffic across the WAN links is minimized.
B.   DNS replication traffic across the WAN link is minimized
C.   DNS replication traffic across the public WAN links is secured.
D.   Name resolution performance for client computers is optimized.

Answer: A, D
Explanation: The clients on each office are configured to use their local DNS server for name resolution, so the DNS name resolution traffic across the WAN links are minimized and name resolution performance for the client are optimized.

Incorrect Answers:
B: DNS replication on the WAN links is not minimized since incremental zone transfers only can be used in Active Directory integrated zones, not in replication between primary and secondary DNS zones.
C: DNS replication on the public WAN links is secure. Active Directory integrated zones would enable secure replication, but replication between primary and secondary DNS zones is not secure.

QUESTION NO: 103
You are the administrator of TestKing's network. The network consists of a single Windows 2000 domain that spans multiple locations. The locations are connected over the Internet by using Routing and Remote Access.

Resources are located on TCP/IP hosts on your network. To facilitate name resolution for client access to these resources, you implement Windows 2000 DNS servers on your network.

You want to ensure that when the zone transfer traffic between your DNS servers crosses the Internet links between the locations, it cannot be compromised by outside parties. What should you do?

A.   Select the option to allow zone transfers only to servers listed on the **Name Servers** tab.
B.   Set up an Active Directory integrated zone.
C.   Set the **Allow Dynamic Updates** setting for your zone to **No**.
D.   Set the **Allow Dynamic Updates** setting for your zone to **Only Secure Updates**

Answer: B
Explanation: Only Active Directory integrated zone transfers will provide secure DNS replication traffic. Active Directory integrated zone transfers are included in Active Directory replication. Active Directory replication use secure channel to make the replication traffic safe from outside parties.

Incorrect Answers:
A: The servers listed on the Name Servers tab are the destinations of the zones transfers. It does not concern the security of the zone transfers.
C: Configuring the **Allow Dynamic Updates** setting to No disables Dynamic DNS, but the zone transfers would still be insecure.
D: Configuring the **Allow Dynamic Updates** setting to Only Secure would make the updates of the DNS zone secure, but the zone transfers would still be insecure.

QUESTION NO: 104
You are the administrator of TestKing's network, which consists of a LAN with 5,000 computers on 15 subnets. Each subnet is a separate network segment. You anticipate that the number of hosts on your network will increase by 10 percent each year for the next three years.

The network includes three Windows 2000 server computers configure as routers. The relevant portion of your existing network configuration is shown in the exhibit.
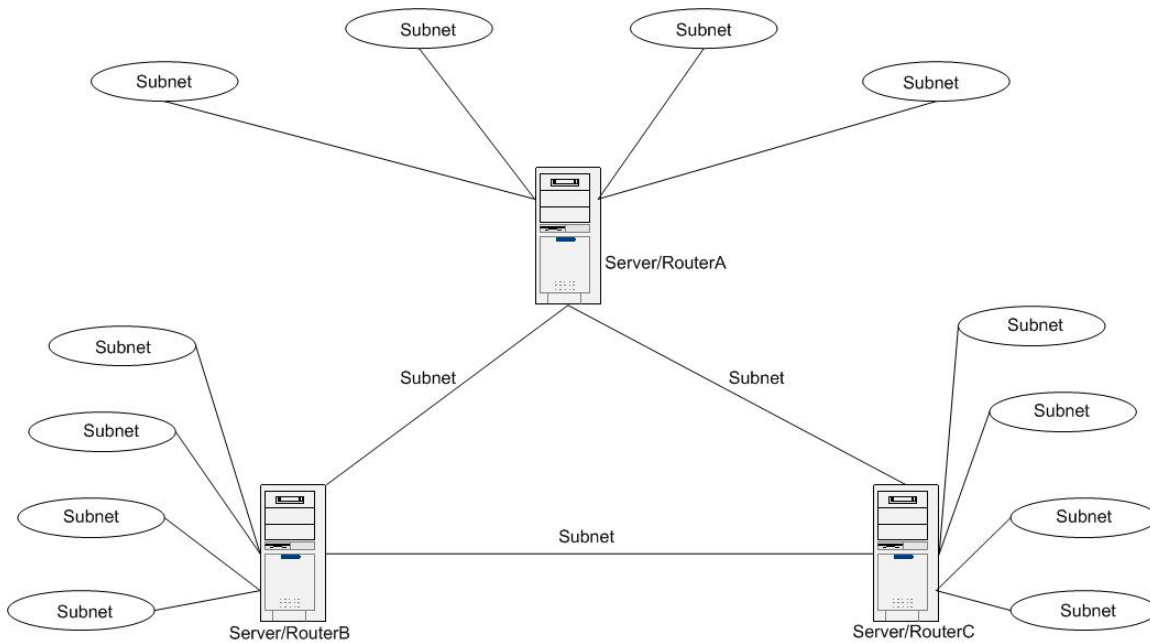
You need to configure the routers so that existing hosts on all subnets can communicate with existing hosts on all other subnets. Your solution must minimize network protocol traffic, and it must allow the subnets to be reconfigured to accommodate the anticipated growth.

What should you do?

A.   Create two additional subnets for each router. Enable Routing and remote access on each router and add the OSPF protocol in a default configuration. Add each network interface on each router to the OSPF protocol.

B.   Reconfigure the routers and network segments in a backbone configuration. Add two additional subnets for each router. Enable routing and remote access on each router and add the OSPF protocol in a default configuration. Add each network interface on each router to the OSPF protocol.

C.   Enable routing and remote access on each router and add RIP in a default configuration. Add each network interface on each router to RIP.

D.   Enable routing and remote access on each router and add RIP, configured to use RIP neighbors instead of broadcast or multicast routing. Add each network interface on each router to RIP.

Answer: B
Explanation: For larger network, like in this scenario, performance of RIP would suffer, mostly because it is based on broadcasts. OSPF on the other hand is designed for large scale networks. OSPF divides the internetwork into different areas – every area is a contiguous network. The areas are connected with each other through a backbone area. The routers connected to the backbone area are called backbone routers.

Incorrect Answers:
A: Areas connecting to each other through backbones, not new subnets on every router, is the way OSPF is set up.

C: OSPF, not RIP, is the preferred routing protocol in larger networks.
D: OSPF, not RIP, is the preferred routing protocol in larger networks.

QUESTION NO: 105
You are the administrator of TestKing's network, which includes a Windows 2000 Server computer named AX1 that runs Routing and Remote Access. You configure remote access policies on AX1 as shown in the following table.

Policy	Order
Weekday 7:00 AM – 6:00 PM: Allow	1
Administrators: Allow	2
Weekday 6:00 P:M – 7:00 A.M: Deny	3
Support Managers: Allow	4
Weekend: Deny	5

Your management revises its access policies. Members of the Support Managers group are now allowed to dial in 24 hours a day, seven days a week. Members of the Administrators group are no longer allowed to dial in on weekends.

To implement these changes, you need to reconfigure the remote access policies on AX1. What should you do?

A.   Move the Weekend: Deny policy directly above your current policy 2.

B.   Move the Support Managers: Allow policy directly above your current policy 3.

C.   Move the Administrators: Allow policy above your current policy 1. Move the Weekday 6:00 P.M. – 7:00 A.M: Deny Policy directly below your current policy 3.

D.   Move the Support Managers: Allow policy above your current policy 2. Move the Weekend: Deny policy directly above your current policy 3.

Answer: D
Explanation:
We must fix two problems in this scenario:
1. The Administrators should no longer be allowed to log in on weekends.
2. The Support Managers must be allowed to login all hours, all days. They are now only allowed to log in Weekdays 7 AM to 6 PM.

We must take into consideration that the Policys are processed in order and the first matching Policy is applied.

Moving the Support Managers: Allow policy above the current policy 2 would ensure that the Support Managers have access all hours, all days.

Moving the Weekend: Deny policy directly above the current policy 3 (at this moment the 3rd policy is the Administrators: Allow policy) would ensure that only the Support Managers would get Weekend access. The rest of the users, including the Administrators would be denied access during the weekend.

Incorrect Answers:
A: If we move the Weekend: Deny policy above the policy 2, everyone would be denied access during the weekends.

B: If we only move the Support Managers: Allow Policy, the Administrators would still be able to log on during weekends.

C: Moving the Administrators: Allow policy to the first spot, would ensure that the Administrators are log on all days, all hours. But they should not have access during the weekends.

QUESTION NO: 106
You are the network administrator for Luceme Publishing. Your company employs a full-time staff. It also contracts authors for short-term projects.

All full-time employees use portable computers running Windows 2000 Professional. These users require remote access to network resources, such as applications and printers. Contracted authors use personal computers that run a variety of operating systems, including Windows 98, Windows NT 4.0, and Windows 2000 Professional. The authors require remote access to the network so they can upload revised documents to file servers. You allow remote access to the network only by means of a virtual private network connection through the Internet.

You configure 40 PPTP ports on a single VPN server. To ensure high availability of the VPN service, you configure three additional VPN servers. You configure 40 L2TP ports on each new server. You configure round robin DNS entries for all four VPN servers.

Several authors now report that they experience rejected connections when they dial the VPN servers. After repeated attempts they are eventually able to connect. Full-time employees report no problems.

You need to correct this problem while ensuring the highest possible level of security for each connection. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

    A.   Configure 40 PPTP ports on each new VPN server
    B.   Configure 40 L2TP ports on the original VPN server
    C.   Remove the 40 PPTP ports on the original VPN server
    D.   Remove the 40 L2TP ports from each new VPN server.
    E.   Remove the dedicated IP address from the server interfaces that receive the VPN connections.
    F.   Remove the round robin DNS entries for the VPN servers and assign users to specific VPN servers.

Answer: A, D
Explanation: In this scenario one VPN server is configured for PPTP, the other three are configured for L2TP. L2TP is supported by Windows 2000, but it is not supported by downlevel clients such as Windows 98 and Windows NT 4.0. When a remote downlevel client connects the connection will only be successful when it uses the VPN server configured for PPTP, that is it is 25% chance of getting a connection. The Windows 2000 remote clients get access either by PPTP or by L2TP.

A: By configuring all VPN server with 40 PPTP ports there would be no problem to get a connection for any author, including the ones using downlevel clients.
D: L2TP is not encrypted unless it is used in connection with IPSec. By removing L2TP from all L2TP ports only secure PPTP connections would be allowed.

Incorrect Answers:
B: L2TP is not secure. Windows 2000 clients which get L2TP connections would have unencrypted connections.
C: The L2TP ports, not the PPTP ports, should be removed. The downlevel clients, Windows 95 or Windows NT 4.0, would not be able to be granted remote access if PPTP ports are removed.
E: The IP address configuration of the server interface has a correct setting. The problem at hand concerns the L2TP protocol.
F: Round robin is working correctly. It is not necessary to change the configuration of round robin.

QUESTION NO: 107
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. Company employees need to access network resources when they are working remotely.

Some remote users work at home, using personal desktop computers that run either Windows 98 or Windows 2000 Professional. The home computers do not have computer accounts in the company's domain. Other remote users have company-issued portable computers that run Windows 2000 Professional. The portable computers have computer accounts in the company's domain. The portable computers also contain a smart card reader, which is the only means of authentication for the employees who use them.

To provide secure access for all remote users, you enable Routing and Remote Access on a Windows 2000 Server computer that is connected to the Internet. You also create ports for 25 PPTP virtual private network (VPN) connections. You verify that all VPN client computers are configured correctly.

To ensure security, you create a single Routing and Remote Access policy for all users and configure authentication as shown in the exhibit. .
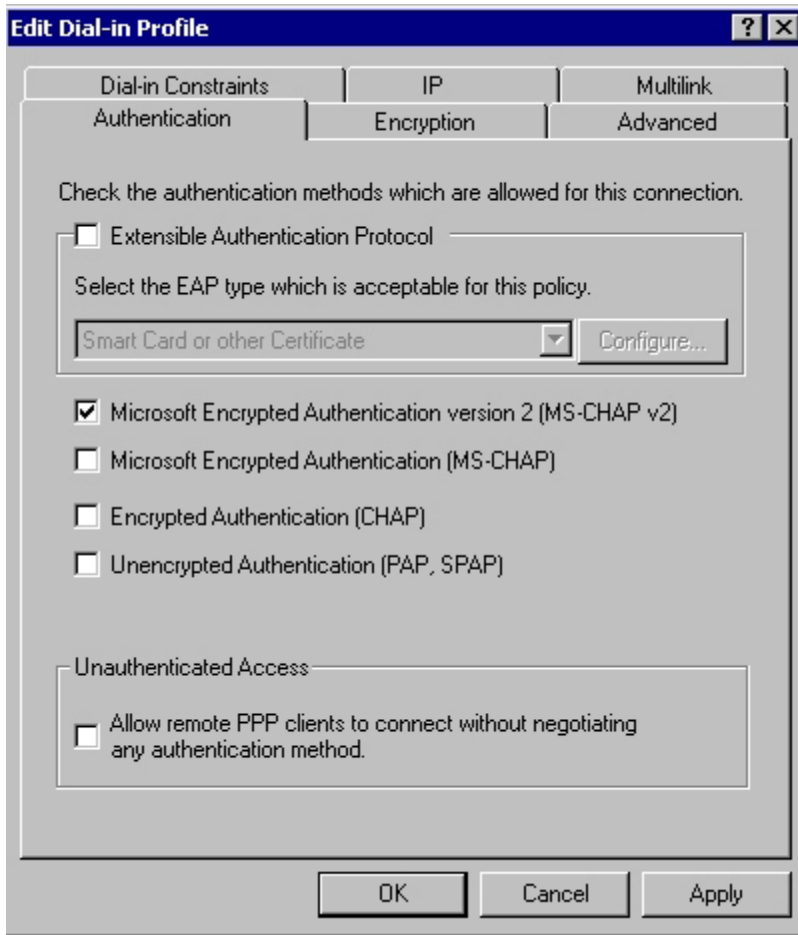
All remote users with desktop computers running Windows 2000 Professional can now successfully connect to the VPN server. However, no other remote users can establish a connection.

You need to enable all remote users to connect to the VPN server. You also need to ensure the highest possible level of authentication security.

Which two actions should you perform in the remote access profile? (Each correct answer presents part of the solution. Choose two)

 A. Create computer accounts for all the home computers
 B. Select the **Extensible Authentication Protocol** check box and select **Smart Card or other Certificate** in the list box.
 C. Select **the Extensible Authentication Protocol** check box and select **MD5 Challenge** in the lost box.
 D. Select the **Microsoft Encrypted Authenticated (MS-CHAP)** check box
 E. Select the **Unencrypted Authentication (PAP, SPAP)** check box.
 F. Clear the **Microsoft encrypted Authentication version 2 (MS-CHAP v2)** check box.

Answer: A, B
Explanation: Select the Extensible Authentication Protocol (EAP) with the Smart Card or other certificate option must be selected since the portable computers have smart card readers as the only means of authentication. Smart card authentication requires computer accounts for all the home computers.

Reference: Microsoft Server Documentation, EAP

Incorrect Answers:
C: MD5 challenge cannot be used since the portable computers have smart card readers as the only means of authentication.
D: Microsoft CHAP would not provide highest possible level of authentication security.
E: Unencrypted Authentication would not provide highest possible level of authentication security.
F: It is not necessary to clear the MS CHAP V2 check box. It is cleared automatically when Extensible Authentication Protocol is selected.

QUESTION NO: 108
You are the administrator of TestKing's network. Your network consists of a single segment, which you divide into four segments by installing routers. The relevant portion of the new network configuration is shown in the exhibit. .

The new configuration includes a DHCP server running Windows 2000 on segment B. Each new segment also includes one client computer running Windows 2000 Professional. These computers are named Client1 through Client4.

Leading the way in IT testing and certification tools, www.testking.com

Segment C and segment D each include one file server running Windows 2000 Server. The file servers are named File1 and File2. You configure the client computers as DHCP clients. You assign static IP addresses to the Windows 2000 Server computers. You create four scopes on the DHCP server with the correct IP addresses.

When you test your configuration, you discover that Client1; Client2, and Client4 cannot communicate with any other computers on the network. Client3 can communicate with File1 and File2, but not with other client computers.

You need to ensure that all client computers can communicate with both file servers and with each other. Which action or actions should you perform? (Choose all that apply)

    A.   Configure Client1 as a DHCP Relay Agent.
    B.   Configure Client2 as a DHCP Relay Agent.
    C.   Configure Client4 as a DHCP Relay Agent.
    D.   Configure File1 as a DHCP Relay Agent.
    E.   Configure File2 as a DHCP Relay Agent.
    F.   Configure Router A to forward BOOTP packets.
    G.   Configure Router B to forward BOOTP packets.

Answer: D, E, F
Explanation: In this scenario apparently the DHCP configuration information are not able to reach the remote subnets. The most likely cause is that the routers are not BOOTP-enabled and blocks this traffic.
D, E: We must ensure that Client1, Client2, and Client4 can communicate with other computers on the network. We already know that File1 and File2 are able to communicate with other computers, in particular with Client3. We could therefore use them as DHCP Relay agents. This will ensure that Client2 and Client4 receive proper IP configuration.
F: We must also ensure that Client1 can work as a DHCP client. We ensure this by configuring RouterA to forward BOOTP packets.

Note: Only Windows 2000 Server computers, not Windows 2000 Professional computers, can be configured as DHCP Relay Agents.

Incorrect Answers:
A: Client1 is not able to function as DHCP Relay agent since it is a Windows 2000 Professional computer.
B: Client2 is not able to function as DHCP Relay agent since it is a Windows 2000 Professional computer.
C: Client4 is not able to function as DHCP Relay agent since it is a Windows 2000 Professional computer.
G: By examining the exhibit, we see that we in order for Client1 to receive IP configuration from the DHCP Server RouterA, not RouterB, must be BOOTP enabled.

Leading the way in IT testing and certification tools, www.testking.com

QUESTION NO: 109
You are the network administrator for a branch office of a large company. Your network is connected to the company network by means of a Windows 2000 routing and remote access two-way demand-dial connection over ISDN. In addition to e-mail and application traffic, sensitive company data is transferred across this connection.

You want to accomplish the following goals:

- **All data transmitted over the connection will be secure.**
- **Rouge routers will be prevented from exchanging router information with either router.**
- **Both routers in the connection will be able to validate each other.**
- **Both routers in connection will maintain up-to-date routing tables.**
- **Traffic over the demand-dial link during peak business hours will be minimized.**

You take the following actions:

- **Enable MS–CHAP as the authentication protocol on both routing and remote access servers.**
- **Enable open shortest path first (OSPF) on the demand-dial interfaces.**
- **Set the Require Encryption option in the Advanced Security settings on both routing and remote access servers.**

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

A.   All data transmitted over the connection is secure.
B.   Rogue routers are prevented from exchanging router information with either router.
C.   Both routers in the connection are able to validate each other.
D.   Both routers in connection maintain up-to-date routing tables.
E.   Traffic over the demand-dial link during peak business hours is minimized.

Answer: A, D
Explanation: MS-CHAP has been enabled as the chosen authentication protocol and it supports data encryption so all data transmitted over the connection is secure.
OSPF has been enabled on the demand-dial interfaces so both routers are able to keep up-to-date routing tables.

Incorrect Answers:
B: OSPF could be configured to prevent rouge router from communicating with the real routers. But this has not been done here.
C: MS-CHAP V2 and EAP-TLS supports two-way authentication. MS-CHAP only provides one way authentication; the routers will not be able to validate each other.
E: Nothing has been done to minimize traffic on the demand-dial link during peak business hours.

QUESTION NO: 110

Leading the way in IT testing and certification tools, www.testking.com

You are the administrator of your Windows 2000 network. The network contains a Windows 2000 Server computer named RouterA. Routing and remote access is enabled as a router on RouterA. RouterA has a LAN interface named Net1. The Net1 interface uses an IP address of 192.168.1.2.

You want to specify which type of network traffic will be allowed into the router through the Net1 interface. The only traffic that should be allowed into the Net1 interface is HTTP uses TCP port 80 or TCP port 443. The other interfaces of the router have no restriction on types of the network traffic allowed.

You configure two input packet filters on the Net1 interface as shown in the following dialogue box.
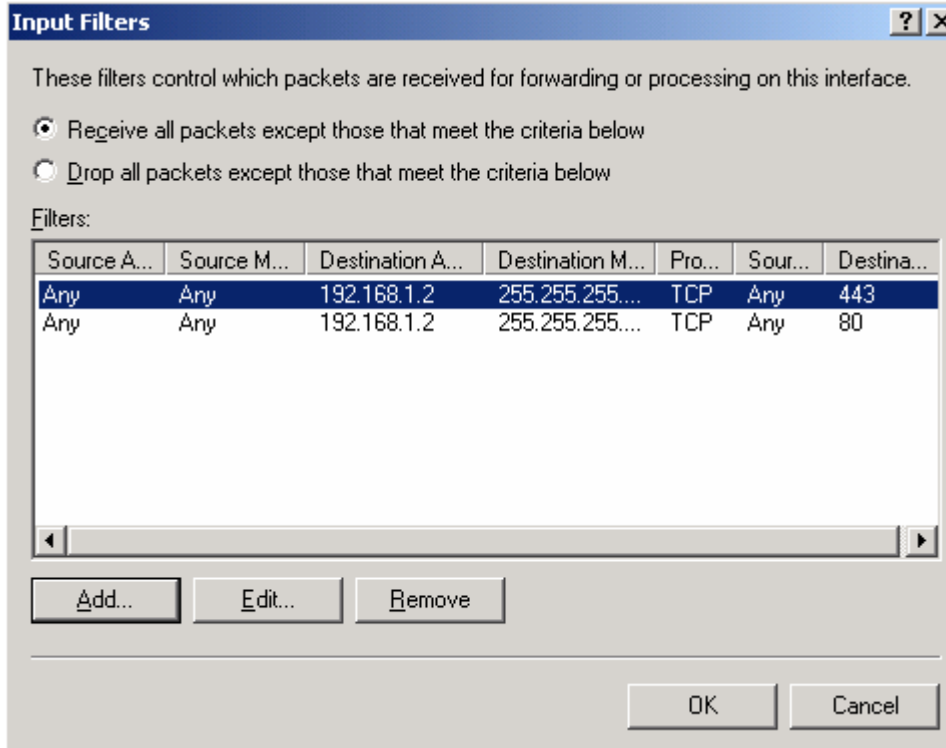
When you move monitor, you notice the other network traffic is still allowed into the router through the Net1 interface.
What should you do?

A. Configure the network connection to use TCP/IP filtering. Permit only TCP port 80 and TCP port 443.
B. Configure the input packet filters to drop all packets except packets allowed by the filters.
C. Configure two output packet filters to filter on both TCP port 80 and TCP port 443.
D. Configure the Net1 interface to drop all UDP packets.

Answer: B
Explanation: By configuring the input packet filters to drop all packets except the packets allowed by the filters, only TCP port 80 and TCP port 443 traffic will be allowed.

Incorrect Answers:
A: To configure the router, the Routing and Remote access console should be used. Not by configuring TCP/IP filtering on the LAN interface.
C: Input filter, not output filters, should be used to decide which traffic should be allowed into the router.
D: The Net Interface should allow only TCP port 80 and TCP port 443. Dropping all UDP packets is not enough.

QUESTION NO: 111
You are the administrator of Windows 2000 network. The network of 85 Windows 2000 Professional computers and two Windows 2000 Server computers named Amsterdam and Utrecht. Amsterdam has a permanent cable modem connection to the Internet.

All Windows 2000 Professional computers on the network are configured to use automatic private IP addressing (APIPA). The network does not contain a DHCP server.

To allow all Windows 2000 Professional computers on the network to access the Internet through the cable modem connection of Amsterdam, you install and configure the network address translation (NAT) routing protocol on Amsterdam.

You decide to use IP addresses in the range of 172.20.20.1 through 172.20.20.150 for the network. Amsterdam is configured to use an IP address of 172.20.20.1.

Utrecht is a web server configured with an IP address of 172.20.20.2 and a default gateway of 172.20.20.1

You want to allow Internet users from outside your internal network to access the resources on Utrecht through the NAT on Amsterdam.

How should you configure the network to accomplish this goal?

   A.   Configure the NAT routing protocol to enable the use of a network application. Specify **web server** as the name of the application. Use the web port number as the remote server port number.
   B.   Configure the public interface of the NAT routing protocol to use an address pool with an address of 172.20.20.2
   C.   Configure the public interface NAT routing protocol to use a special port that maps to the web server port and an IP address 172.20.20.2
   D.   Configured Amsterdam so that it has a static route on the private network. Use a destination address of 172.20.20.2, a network mask of 255.255.255.255, and a gateway of 172.20.20.1

Answer: C.
Explanation: When using the NAT routing protocol we have to use port mappings to give external Internet users access to local resources. If multiple private addresses are mapped to a single public address, as seems to

be the case in this scenario, NAT uses dynamically chosen TCP and UDP ports to distinguish one intranet location from another.

Incorrect Answers:
A: Network application is not used to give external users access to local resources.
B: The public interface cannot use private addresses.
D: We do not configure static routes on the private network to enable external access of internal resources.

QUESTION NO: 112
You are the administrator of a Windows 2000 network. The network consists of a Windows 2000 Server computer named ServerA and 50 Windows 2000 Professional computers. ServerA has a dial-up connection that connects to the Internet.

All Windows 2000 Professional computers in the network are configured to use Automatic Private IP addressing (APIPA). There is no DHCP server on the network.

To allow all Windows 2000 Professional computer on the network to access the Internet through the dial-up connection of ServerA, you decide to install the network address translation (NAT) routing protocol.

You configure ServerA as follows:

- **The LAN interface on ServerA has an IP address of 10.65.3.1 and a subnet mask of 255.255.255.0**
- **NAT automatically assign IP addresses in the range of 10.65.3.2 through 10.65.3.60 to computers on the private interface.**
- **NAT uses a demand-dial interface named Dial ISP to connect to the Internet service provider.**
- **The Dial ISP interface uses an address spool in the range of 207.46.179.44 through 207.46.179.36**
- **The routing table has a default static route for the public interface.**

Which configuration should you use for the static route for the public interface?

    A.   Interface: local area connection
           Destination: 207.46.179.33
           Network Mask: 255.255.255.255
           Gateway: 0.0.0.0
    B.   Interface: local area connection
           Destination: 10.65.3.0
           Network Mask: 255.255.255.0
           Gateway: 10.65.3.1
    C.   Interface: Dial ISP
           Destination: 0.0.0.0
           Network Mask: 0.0.0.0
           Gateway: None
    D.   Interface: Dial ISP

Destination: 207.46.179.32
Network Mask: 255.255.255.240
Gateway: 207.46.179.32

Answer: C.
Explanation: For a default static route, we need to select the demand-dial interface (for dial-up connections) or LAN interface (for permanent or intermediate router connections) that is used to connect to the Internet. The destination is 0.0.0.0 and the network mask is 0.0.0.0. For a demand-dial interface, the gateway IP address is not configurable.

Incorrect Answers:
A: Destination and network mask has to be 0.0.0.0
B: Destination and network mask has to be 0.0.0.0
D: Destination and network mask has be 0.0.0.0

QUESTION NO: 113
You are the administrator of TestKing's network. To allow users to access network resources when they are not in the office, you configure remote access services in their native mode Windows 2000 domain. Because your company operates 24 hours a day and seven days a week, and because your users are not running Windows 98 and Windows NT workstation, you do not want to apply any time or authentication restrictions. To accomplish this, you delete the default remote access policy. However, you want to restrict access by unauthorized users.

You grant all users in the domain to allow access dial-in permission, but you begin to receive reports that users are not able to receive the connection.

What should you do to resolve the problem?

   A.   Create a new remote access policy that has the condition to grant all members of the domain users group dial-in access.
   B.   Create a new group policy that grants dial-in permissions to the domain user group.
   C.   Edit the remote access profile to allow the use of encrypted authentication (CHAP) as the only authentication method.
   D.   Edit the remote access profile to allow the users of unencrypted authentication (PAP, SPAP) as the only authentication method.

Answer: A
Explanation: The access to a RRAS server is through the combination of the user's Dial-in permissions; Remote Access Policy, which specifies various conditions for permitting a condition; and Remote Access Profiles, which determines what kind of access that RRAS grants if a connection is permitted. In this scenario the dial-in permission is set to Allow for all users in the native domain. Still a remote access policy must allow

the users to get access. The default remote access policy has been deleted so a new one has to be created. By setting the condition to grant all members of the domain users group access, only authorized domain users will be granted remote access.

Incorrect Answers:
B: Group policies cannot be used to grant remote access.
C: Remote access profiles cannot grant remote access, they can only be used to decide which kind of access a user would after access has been granted.
D: Remote access profiles cannot grant remote access, they can only be used to decide which kind of access a user would after access has been granted.

QUESTION NO: 114
You are the network administrator of a Woodgrove bank. Woodgrove bank needs records of every one who will access company's network by routing and remote access. You are configuring the routing and remote access server for remote access.

You need to log all logon activity on the routing and remote access server. What should you do?

   A.   In the Audit Policy for the domain, enable Directory Service Access.
   B.   In the Audit Policy for the domain, enable Audit Logon Events.
   C.   In the Audit Policy for the domain, enable Audit Account Logon Events.
   D.   On the Routing and Remote Access server, enable log authentication requests in the Remote Access Logging properties.
   E.   On the Routing and Remote Access server, enable log accounting requests in the remote access logging properties.

Answer: D
Explanation: The Log authentication requests option can help by alerting us to problems with transaction volume and of unauthorized attempts to access resources. To enable Log Authentication requests we must open the Routing and Remote Access console and click Remote access logging in the console tree. In the details pane, right-click Local File, and then click Properties. Select the Settings tab, select one or more check boxes for recording authentication and select the Log authentication requests check box.

Incorrect Answers:
A: This setting is configured in the Routing and Remote access console, not in the audit policy for the domain
B: This setting is configured in the Routing and Remote access console, not in the audit policy for the domain
C: This setting is configured in the Routing and Remote access console, not in the audit policy for the domain
E: The Log authentication requests, not the Log accounting requests, should be selected.

QUESTION NO: 115
You are the administrator of TestKing's network. You need to implement a remote access solution that is highly available and highly secure. Your company consists of a single location and has a T3 connection to the Internet.

Your company has 1,000 salespeople who need reliable connectivity to the company network from any remote location. All servers are running Windows 2000 Advanced Server, and all client computers are running Windows 2000 Professional.

You want to accomplish the following goals:

- **No single point of failure, aside from total loss of the T3, will result in total loss of remote access connectivity.**
- **No authentication traffic will be carried as clear text.**
- **No data traffic will be carried as clear text.**
- **Support for at least 200 simultaneous remote users accessing the network will be available at all times.**

You take the following actions:

- **Install three virtual private network (VPN) servers at the main office.**
- **Configure each VPN server to support 150 PPTP connections.**
- **Configure the client computers to use Password Authentication Protocol (PAP) as the authentication protocol.**

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

    A.   No single point of failure, aside from total loss of the T3, results in total loss of remote access connectivity.
    B.   No authentication traffic is carried as clear text
    C.   No data traffic is carried as clear text
    D.   Support for at least 200 simultaneous remote users accessing the network is available at all times

Answer: A, D.
Explanation: Three VPN servers have been installed at the main office. This provides redundancy.
The three VPN servers provide 150 connections each. 450 simultaneous connections are supported. Even if one VPN is stopped 300 simultaneous connections will still be provided.

Incorrect Answers:
B: PAP uses no encryption for authentication. The authentication traffic is sent in clear text.

Leading the way in IT testing and certification tools, www.testking.com

C: PPP encryption requires either EAP-TLS, MS-CHAP or MS-CHAP v2 in combination with Point-to-Point Encryption (MPPE) to encrypt data. PPP does not provide data encryption.

QUESTION NO: 116
You are the administrator of TestKing's network. The company's Internet web server runs on Windows 2000 Server computer. The web server is not a member of domain and you want to keep the web server separate from the rest of your network.

Your company wants its customers to be able to connect to the web sever to make online transactions. You want to ensure that these transactions are secured through encryption. You also want to assure customers of the identity of your web server when they make online transactions.

What should you do?

  A. Install an enterprise certificate authority.
  B. Install a subordinate enterprise certificate authority that uses a commercial CA as the parent.
  C. Install a stand-alone certificate authority.
  D. Install a subordinate stand-alone certificate authority that uses a commercial CA as the parent.

Answer: D
Explanation: The web server is not a member of the domain and it is kept separate from the rest of the network. The Certificate Authority (CA) should therefore not be a part of the domain; it should not be an Enterprise CA or a subordinate Enterprise CA. The CA must be a subordinate CA to commercial CA so that the external customers can connect to the commercial and get certificates that verify the authenticity of your web server.

Incorrect Answers:
A: The CA of the web server should not be a part of the domain. It should not be an enterprise certificate authority.
B: The CA of the web server should not be a part of the domain. It should not be a subordinate enterprise certificate authority.
C: The external customers must be able to connect to the CA. The CA cannot be a stand-alone CA; it must use a commercial CA as its parent.

QUESTION NO: 117
You are the administrator of TestKing's network, which uses TCP/IP as its only network protocol. The network uses the private address space of 192.168.1.0/24.

To improve performance, you decide to segment the network as shown in the exhibit.

Leading the way in IT testing and certification tools, www.testking.com
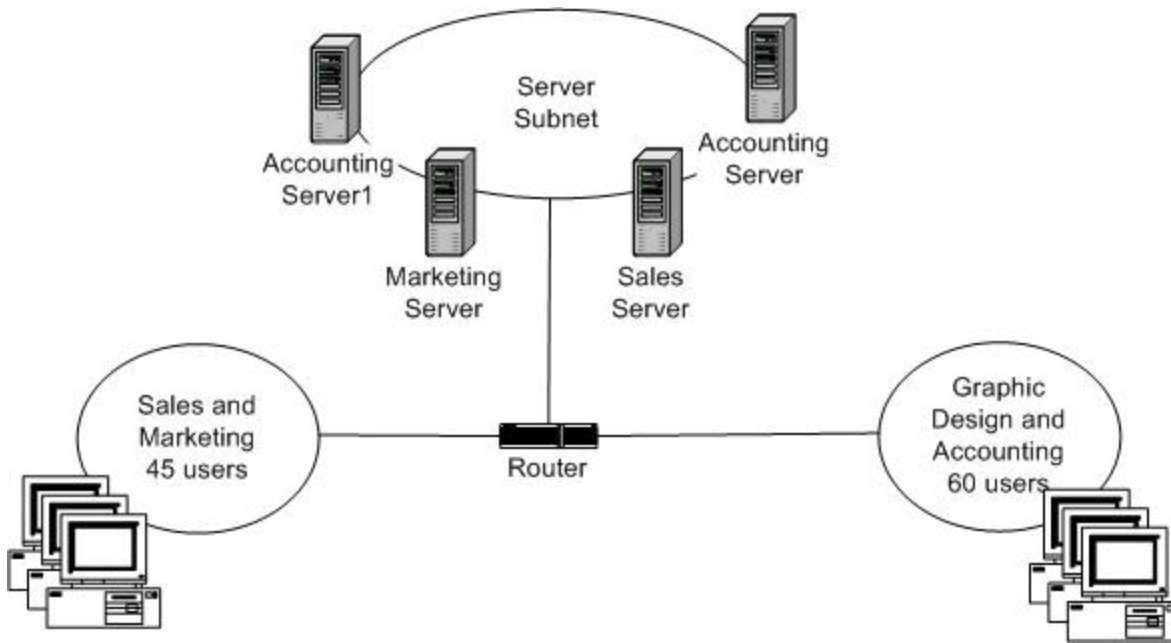
Now you need to configure a subnet mask for the entire network. Which subnet mask should you configure?

A. 255.255.255.0
B. 255.255.255.128
C. 255.255.255.192
D. 225.255.255.224
E. 255.255.255.240

Answer: C
Explanation: We require 3 subnets, and a maximum of 60 hosts on each subnet. With subnet mask 255.255.255.192 we would have four subnets, with 62 clients on each:
192.168.1.0/26
192.168.1.64/26
192.168.1.128/26
192.168.1.192/26

Note: Cisco and Microsoft do not use the same formula to calculate the number of possible subnets:
Microsoft: Number of subnets: 2^number-of-subnet-bits
Cisco: Number of subnets: 2^number-of-subnet-bits – 2
For example, Cisco would say that a subnet mask of 255.255.255.192 only gives two subnets, not four. Actually Cisco routers can handle all four subnets, it is just that on the Cisco exams you should answer two subnets.

Reference: Understanding TCP/IP Addressing and Subnetting Basics (Q164015)

Leading the way in IT testing and certification tools, *www.testking.com*

Incorrect Answers:

A: Would only allow use to use one subnet, which makes the router useless.

B: Would allow 2 subnets with 126 clients each.

D: Would only allow 30 clients on each subnet.

E: Would only allow 14 clients on each subnet.

QUESTION NO: 118
You are the administrator of a Windows 2000 network. The network consists of a single domain that has three Windows 2000 domain controllers, 1000 Windows and 2000 Professional workstations.

Your company wants to make use of digital certificates by installing its own certificate authority (CA). You want to protect the root CA and the private key. You also want to ensure that you are able to effectively manage TestKing's public key infrastructure.

You want to accomplish the following goals:

- **The server that is hosting the root CA will have a maximum amount of protection from any security breaches that could occur on the network.**
- **The server that is hosting the root CA will be able to certify other CAs and revoke certificates.**
- **All the servers in your domain will be able to access the revocation status of all certificates in your public key infrastructure.**
- **Certificate requests by users or computers in the domain will immediately be processed and either granted or denied.**

You take the following actions.

- **On a member Windows 2000 Server computer connected to the network, install a stand-alone root CA.**
- **Disconnect the server on which you install the stand-alone root CA from the network and place it in a secure and separate location.**

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

A.   The server that is hosting the root CA has maximum amount of protection from any security breeches that can occur on the network.

B.   The server that is hosting the root CA is able to certify other CAs and revoke certificates.

C.   All the servers in your domain are able to access the revocation status of all certificates in your public key infrastructure.

D.   Certificate requests made by users or computers in the domain are immediately processed and either granted or denied.

Answer: A
Explanation: In this scenario the CA is very well protected since it is disconnected.

Reference: HOW TO: Install a Windows 2000 Certificate Services Offline Root Certificate Authority (Q271386)

Incorrect Answers:
B: The root CA is disconnected and will not be able to certify other CAs or revoke certificates.
C: The root CA periodically publishes a certificate revocation list (CRL). Programs check the CRLs for all the CAs in the chain of certificates from the end entity to the root of the hierarchy to decide whether or not to trust a particular certificate. The location of the CRL is always included in the certificate in a field called the CRL Distribution Point (CDP). In this case, the root CA in the hierarchy is offline, so the root certificate must be modified to include a CDP that is accessible by users on the network. However, in this scenario no CDP has been created and no revocation status can be accessed.
D: The root CA is disconnected and certificates requests will not be made immediately. In fact the will not processed at all since no CRL Distribution Point (CDP) has been defined (see C.)

QUESTION NO: 119
You are configuring a Windows 2000 server computer on TestKing's network. The network consists of Windows 2000 server computers and NetWare 4.1 servers on two separate subnetworks, as shown in the exhibit. .
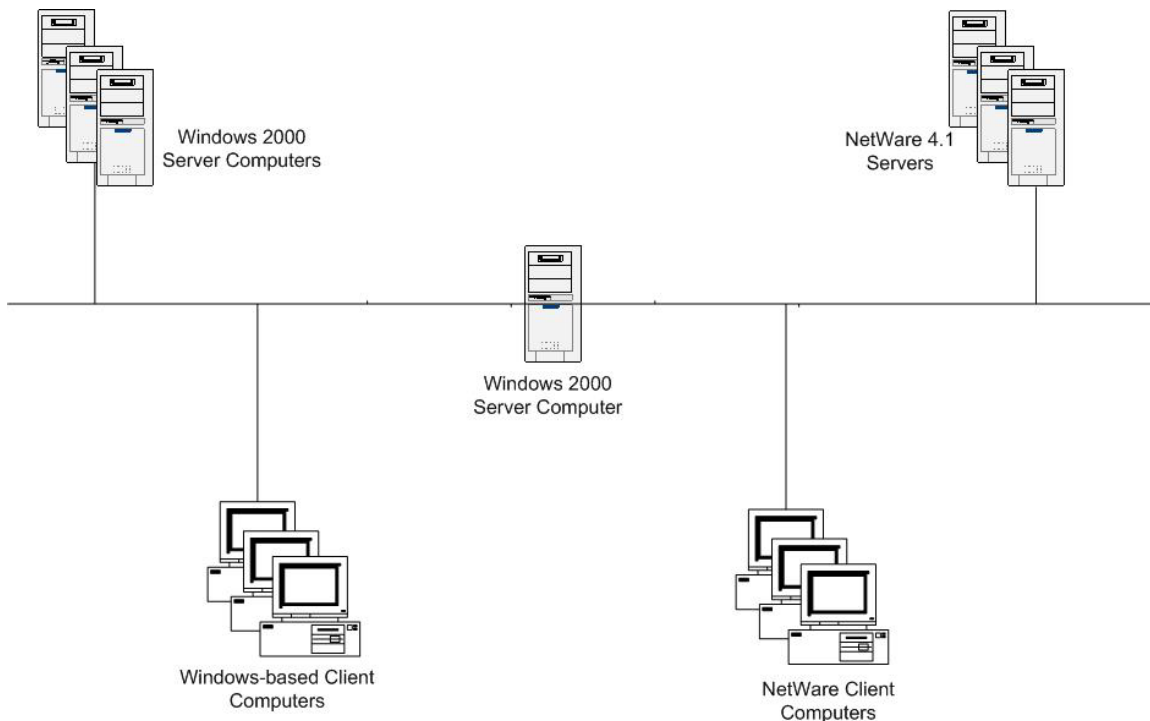
On the subnetwork1, you want Windows 2000 server computers to provide file and print services to Windows-based client computers that use TCP/IP. On subnetwork2, you want the Windows 2000 server computer to provide application services to NetWare client computers that use strictly IPX/SPX. The Windows 2000 server computer has two network adapter cards installed. The Windows 2000 server computer will not function as a router for either subnetwork.

You want to configure the Windows 2000 server computer to provide services on both subnetworks. You also want to optimize network performance for the Windows 2000 server computer and ensure that the response time for both server and client services is minimized.

What should you do? (Choose Two)

A. Configure the network bindings on the Windows 2000 server computer to unbind TCP/IP to the adapter connected to the subnetwork1.
B. Configure the network bindings on the Windows 2000 server computer to unbind NWlink to the adapter connected to the subnetwork1.
C. Configure the network bindings on the Windows 2000 server computer to unbind TCP/IP to the adapter connected to the subnetwork2.
D. Configure the network bindings on the Windows 2000 server computer to unbind NWlink to the adapter connected to the subnetwork2.
E. Configure a unique internal network number for each subnetwork on the Windows 2000 server computer.

Answer: B, C
Explanation: In this scenario network performance should be optimized. A good practice is to remove unused protocols from the network adapters since every installed network protocol brings some overhead. On subnetwork1 the only network protocol used is TCP/IP. Therefore the NWLink protocol should be unbound on the adapter connected to the subnetwork1 on Windows 2000 router computer. On subnetwork2 the only network protocol used is NWLink. Therefore the TCP/IP protocol should be unbound on the adapter connected to the subnetwork2 on Windows 2000 router computer.

Incorrect Answers:
A: TCP/IP is used by the clients on the subnetwork1. On the router the TCP/IP protocol must not be removed on the adapter connected to the subnetwork1.
D: NWLink is used by the clients on the subnetwork1. On the router the NWLink protocol must not be removed on the adapter connected to the subnetwork1.
E: Internal network numbers are needed on networks with two or more NWLink subnets were either FPNW or IPX routing is running. This is not the case here.

QUESTION NO: 120
You are the network administrator for your company. Your company has three networks connected by a router. The router is configured as follows:

Interface0-subnet0-IPAddress172.30.4.1SubnetMask255.255.255.0
Interface1-subnet1-IPAddress172.30.5.1SubnetMask255.255.255.0
Interface2-subnet2-IPAddress172.30.6.1SubnetMask255.255.255.0

Only subnet 1 and subnet 2 contain client computer. Subnet 1 and subnet 2 each contain a Windows 2000 DHCP server, which is responsible for assigning addresses to client computers on the local subnet. The scopes are configured as shown in subnet 1 scope properties and Subnet 2 scope properties as shown in the exhibit. .
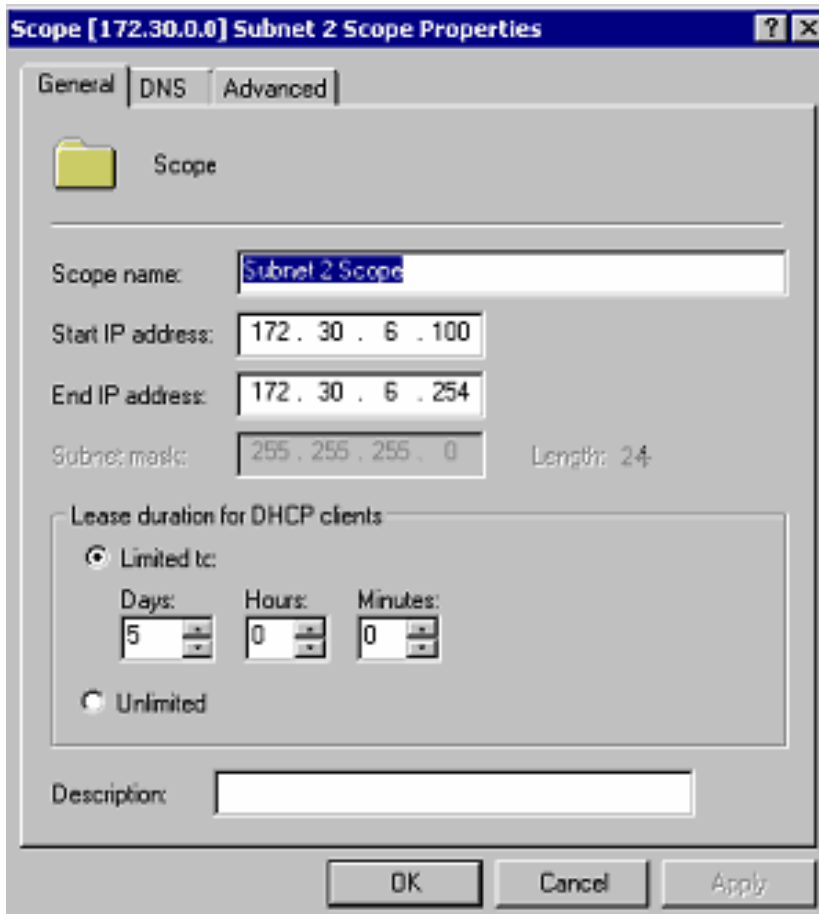
Subnet 0 contains a web server and provides connectivity to the Internet. Users are experiencing connectivity problems. Computers on subnet1 can communicate with any host on their own subnet, but cannot communicate with hosts on Subnet 0 or Subnet 2. Computers on Subnet2 cannot communicate with hosts on subnet 1, but they are not experiencing any problems with connectivity to subnet 0.

What should you do to correct this problem?

    A.   Modify the routing tablets on the router to enable routing from subnet 1 to subnet 0 and subnet 2.

    B.   Modify the routing tablets on each host on subnet 1 to enable direct connectivity to hosts on subnet 0 and subnet 2.

    C.   Delete and re-create the scope on the DHCP server on subnet 1 to reflect the correct subnet mask.

    D.   Delete and re-create the scope on the DHCP server on subnet 2 to reflect the correct subnet mask.

    E.   Delete and re-create the scopes on the both DHCP servers to reflect the same configuration information for each subnet.

Answer: C

Explanation: In this scenario there is a network communication problem. Clients1 on subnet 1 are able to communicate with each other but they cannot connect to resources on the other subnets. Clients on subnet2 can connect to all computers except the ones on subnet 1.
The conclusion is that all the clients on subnet 1 have an incorrect IP configuration. They are all DHCP clients so the DHCP server has been configured incorrectly. By looking at the exhibit we see that the subnet mask of scope1 is 255.255.0.0 but according the configuration of the routers it should have the subnet mask of 255.255.255.0.

Incorrect Answers:
A: The routing table should not be changed. It has the correct information. Every client, except the ones on subnet 1, has proper network access.
B: The routing table should not be changed. It has the correct information. Every client, except the ones on subnet 1, has proper network access.
D: The clients on subnet 2 work correctly. There is no point in changing the scope of the DHCP server on subnet 2.
E: Only the scope1, not both the scopes, has to be changed.

QUESTION NO: 121
You are the administrator of TestKing's network. You are configuring your Windows 2000 network to support a Simple Network Management Protocol (SNMP) management application. Your network is configured as shown in the exhibit.
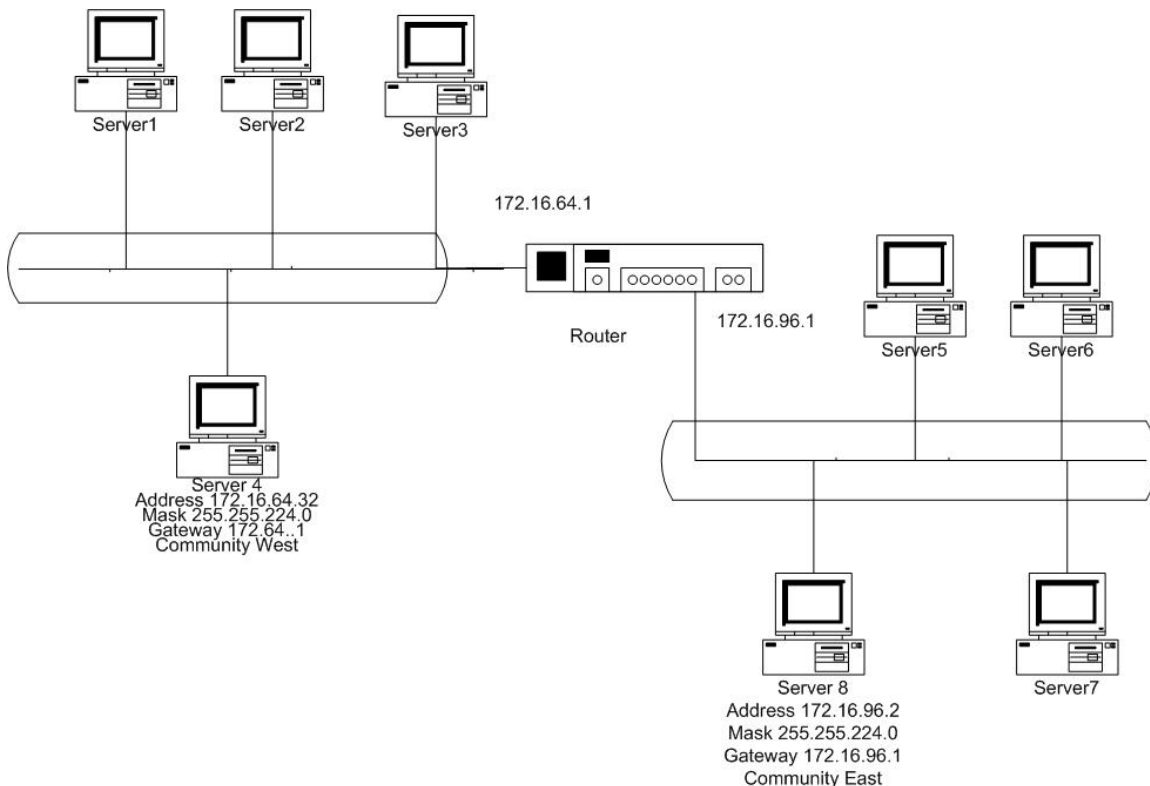
Your SNMP management application is installed on server8. The application can successfully manage all computers except the servers in the west.com domain have the identical SNMP settings.

You need to successfully manage all computers from your SNMP management application. What should you do?

    A.   Join server1, server2, server3, and server4 to the east.com domain
    B.   Establish a trust relationship that allows the west.com domain to trust the east.com domain
    C.   Configure all servers so that they have the same community name
    D.   Set the send authentication trap property to 172.16.96.1 on all servers in west.com domain

Answer: C
Explanation: In this scenario the servers have different community names. To able to communicate within SNMP they must have the same community name. Therefore we must configure all servers so that they have the same community name. We can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administration. Communities are identified by community names that we assign. A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

Incorrect Answers:
A: Joining the server to same domain will not solve the problem. The community names but the same.
B: Explicit trust relationships were used in Windows NT 4.0. It is not necessary to apply them here between two Windows 2000 domains.
D: When an SNMP agent receives a request that does not contain a valid community name or the host sending the message is not on the list of acceptable hosts, the agent can send an authentication trap message to one or more trap destinations.
    Authentication traps cannot be configured to send traps to particular servers based on either IP address or domain. The traps are only sent to servers with a valid community name.

QUESTION NO: 122
You are the administrator of Windows 2000 network. You want to create a DHCP scope for the 192.168.1.32/28 subnet. The computers on this subnet are running Windows 95, Windows 98 and Windows 2000. You also have two UNIX computers on this subnet that will static IP addresses. These UNIX computers will be assigned the two highest available IP addresses on the subnet. The subnet's default gateway will be assigned the lowest available IP address on the subnet. The scope should only include the available addresses.

Which scope should you create on your DHCP server for this subnet?

    A.   192.168.1.34-192.168.1.46.

B. 192.168.1.34-192.168.1.44.
C. 192.168.1.33-192.168.1.45.
D. 192.168.1.34-192.168.1.61.
E. 192.168.1.33-192.168.1.60.

Answer: B
Explanation: From 192.168.1.32/28 we see that the subnet has 28 bits.
Subnet mask in binary: 11111111.11111111.11111111.11110000
The first IP address of the subnet is 192.168.1.32
The last IP address of the subnet 192.168.1.32 + 0.0.0.15 = 192.168.1.32.47
If we analyze the subnet in more detail we get:
192.168.1.32 (Subnet Address, always reserved – cannot be used) (All 0's in host range)
192.168.1.33 (Lowest available IP, reserved for Gateway
192.168.1.34-44 (available host IP addresses which can be used in the scope)
192.168.1.45-46 (highest 2 IP addresses, which are reserved for the Unix machines)
192.168.1.47 (Broadcast address, always reserved – cannot be used) (All 1's on host range)
And we se that range 192.168.1.34-44 can be used for hosts. The DHCP scope must be defined for this range.

Incorrect Answers:
A: This scope includes 192.168.1.45 and 192.168.1.46 that should be reserved for the UNIX machines.
C: This scope includes 192.168.1.45 that should be reserved for one of the UNIX machines. The scope also includes 192.168.1.33 that should be reserved for the default gateway).
D: The highest available IP address of this subnet is 192.168.1.47 not 192.168.1.61.
E: The highest available IP address of this subnet is 192.168.1.47 not 192.168.1.61. The scope also includes 192.168.1.33 that should be reserved for the default gateway).

QUESTION NO: 123
You are the administrator of TestKing's network. The network is configured as shown in the Exhibit. .
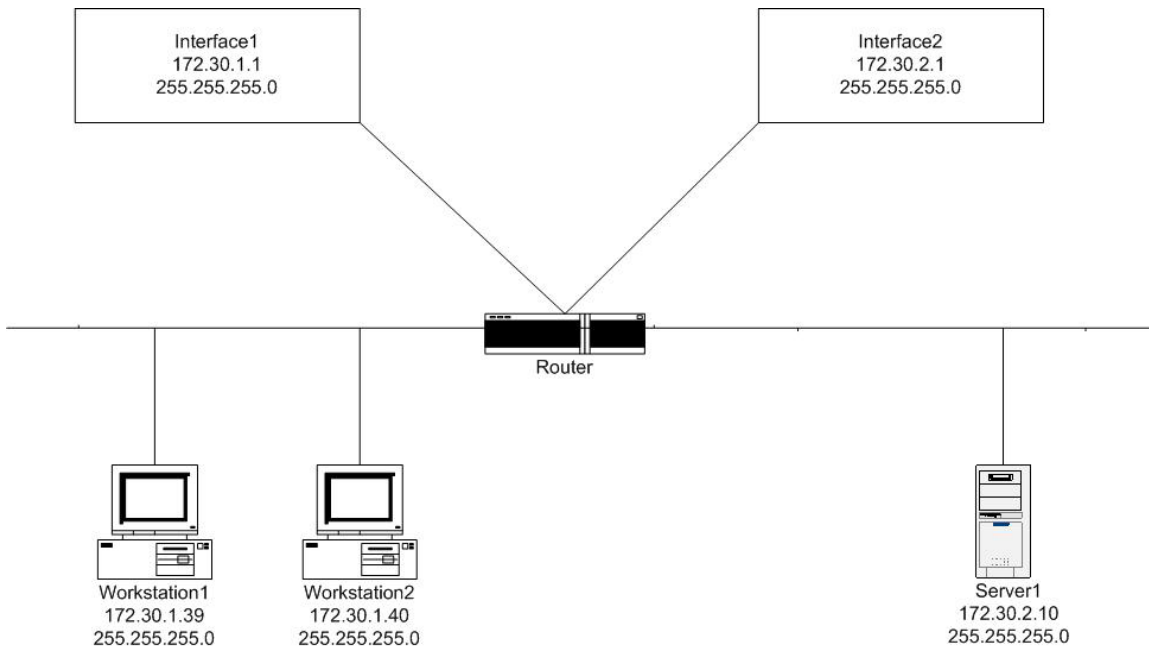
The user of the Workstation1 reports that he cannot access the resources on Server1. You discover that Workstation1 can communicate with any host on its own subnet. You also discover that you can ping the router successfully. You cannot however, communicate with or ping the hosts on the second subnet. Workstation2 is not experiencing any problems.

You run the route print command on Workstation1 and see the following screen output.

```
Active Routes:
Network destination           NetMask  Gateway Interface
Metric
0.0.0.0          0.0.0.0      172.30.1.39172.30.1.39
1
127.0.0.0        255.0.0.0    127.0.0.1  127.0.0.1
1
172.30.1.0       255.255.255.0        172.30.1.39  172.30.1.39
1
172.30.1.39      255.255.255.255      127.0.0.1 127.0.0.1
1
172.30.255.255   255.255.255.255      172.30.1.39  72.30.1.39
1
224.0.0.0        224.0.0.0    172.30.1.39172.30.1.39
1
255.255.255.255 255.255.255.255       172.30.1.39  172.30.1.39
1
```

What should you configure to resolve the communication failure at Workstation1?

A.   The subnet mask on Workstation1.
B.   The subnet mask on Server1.
C.   The default gateway parameter at Workstation1.
D.   The default gateway parameter at Server1.

Answer: C
Explanation: The third column shows the default gateway. Here it only shows loopback address (127.0.0.1) and the address of Workstation1 itself (172.30.1.39), not the correct Default Gateway address. This is also confirmed by the fact the Workstation1 is able to communicate only with computers on its own subnet. We should thus configure the default gateway parameter at Workstation1

Incorrect Answers:
A: Workstation1 is able to communicate only with computers on its own subnet – there is nothing wrong with its subnet mask.
B: The Workstation1 has an incorrect default gateway setting that should be changed, not the subnet mask of Server1.
D: The Workstation1, not the server, has an incorrect default gateway setting that should be changed.

QUESTION NO: 124
You are the administrator of TestKing's network. The network uses TCP/IP exclusively as its transport protocol. The network does not require connectivity to the internet. You are using the address 172.30.0.0/16 for the network.

To improve performance and accommodate recent company growth, you need to develop a strategy to segregate portions of the network. Your initial plan calls for 25 subnets with a maximum of 1,000 hosts per subnet. However, projected growth for the company over the next year indicates a need for at least 55 subnets with maximum of 1,000 hosts per subnet.

Which subnet mask should you configure to meet both the current and future needs of your network?

A.   255.255.240.0.
B.   255.255.248.0.
C.   255.255.252.0.
D.   255.255.254.0.
E.   255.255.255.0.

Answer: C
Explanation: The subnet mask must support minimum 1000 host per subnet and at least 55 subnets.
1000 hosts per subnet indicate that at least 10 bits ($2**9=512 < 1000 < 1024=2**10$) for the hosts. This leaves 22 (32-10) bits for the subnet mask.
Subnet mask, binary: 11111111. 11111111. 11111100.00000000

Leading the way in IT testing and certification tools, www.testking.com

Subnet mask, decimal: 255.255.252.0
We should also check that this subnet mask accommodates for at least 55 subnets. 172.30.0.0/16 is used for the network and the host requires 10 bits, which leaves 6 (32-16-10) for the subnets. This allows 62 (2**6-2) subnets which works fine.

Incorrect Answers:
A: The subnet mask 255.255.240.0 would allow 4094 (2*12-2) hosts, and 14 (2**4-2) subnets. At least 55 subnets was the requirement.
B: The subnet mask 255.255.248.0 would allow 2046 (2*11-2) hosts, and 30 (2**5-2) subnets. At least 55 subnets was the requirement.
D: The subnet mask 255.255.255.0 would allow 254 (2*8-2) hosts, and 254 (2**8-2) subnets. At least 1000 hosts was the requirement.

QUESTION NO: 125
You are the administrator of TestKing's network. Your company wants to analyze ISO and TP4 communications to the Microsoft Exchange Server computer on your network.

To analyze this information, you install Network Monitor on a Windows 2000 Server computer located on the same segment as your Exchange server computer.

How should you configure network Monitor? (Choose two)

    A.   Change the Temporary Capture Directory.
    B.   Copy ISO.dll and TP4.dll to Netmon Subdirectory.
    C.   Copy ISO.dll and TP4.dll to Netmon\Parsers Subdirectory.
    D.   Modify the Parser.ini.
    E.   Modify the Netmon.ini.

Answer: C, D
Explanation: To configure Network monitor to monitor a Microsoft Exchange server we must first copy the Iso.dll, Iso.ini, Tp4.dll files to our NetMon\Parsers subdirectory, these files are located in the BackOffice Resource Kit. We must then make some modifications to the Parser.ini file, the Parser.ini file is located in the NetMon directory.

Reference: How to Install ISO and TP4 Parser for Network Monitor (Q168862)

Incorrect Answers:
A: The temporary directory does not have to be changed.
B: The files ISO.dll and TP4.dll should be copied to Netmon\Parsers Subdirectory, not to the Netmon Subdirectory.
E: The Parser.ini file, not the Netmon.ini file, should be modified.

QUESTION NO: 126
You are the administrator of TestKing's network. Your network is configured to use DHCP to automate the TCP/IP configuration of client computers on your network. All client computers are running Windows 2000 Professional.

To provide router and DNS server information to the client computers, you configure options at the scope level. Your network has certain computers that always require specific address and configuration. You configure reservations in your scope for these computers.

Your Internet service provider (ISP) brings a new router online, which changes your Internet gateway. You reconfigure your scope options to reflect the new router address.

Users of the computers that have the reserved addresses report that they can no longer gain access to Internet, even after they have restarted their computers.
Which two actions should you take to resolve the problem? (Choose Two)

    A.   Use the **ipconfig/release** command at each client computer.
    B.   Use the **ipconfig/renew** command at each client computer.
    C.   Configure the scope options to include the **perform router discovery** button.
    D.   Configure the server option to include the **perform router discovery** option.
    E.   Configure the options on each address reservation to include the new router information.

Answer: B, E
Explanation: After reconfiguring the scope options for the reserved addresses, you need to renew the IP configuration on the client computers.
The Router address, the default gateway, has changed. The IP configuration of the computers has to be changed. This will be done in the following three places:

- at the computers with static IP addresses. You have to do it manually on each of these computers. (this is not listed as an alternative in the question).
- at the DHCP server you must configure the ROUTER information which the DCHP server will provide the DHCP clients. This is already been done for the scope option, but to for the option on each address reservation.
- the DHCP clients, the ones with reserved IP addresses, must get the new DCHP information. This can be done by ipconfig /renew command or by restarting the computers.

Note 1: When you use ipconfig /renew, all network adapters on the computer that uses DHCP (except those that are manually configured) try to contact a DHCP server and renew their existing configuration or obtain a new configuration.
Note 2: To configure the ROUTER option for the reserved IP addresses follow these steps: From the Administrative Tools folder, open DHCP console, select Scope, select Reservations, Right click one Reservation, choose Configure options, select the General Tab (if not chosen), Enable 003 Router, and at Data entry enter either Gateway name or Gateway IP address of the router.

Leading the way in IT testing and certification tools, www.testking.com

Incorrect Answers:
A: Ipconfig/release would just release the current TCP/IP configuration. The client would have no TCP/IP configuration.
C, D: Performed Router Discovery specifies whether the client solicits routers using the router discovery method in RFC 1256". It does not apply. We just have to configure the correct default gateway.

QUESTION NO: 127
You are the administrator of TestKing's network. The company has 60 client computers configured as Proxy client computers. To offer IP addresses to these client computers, your network has one DHCP server as shown in the window.
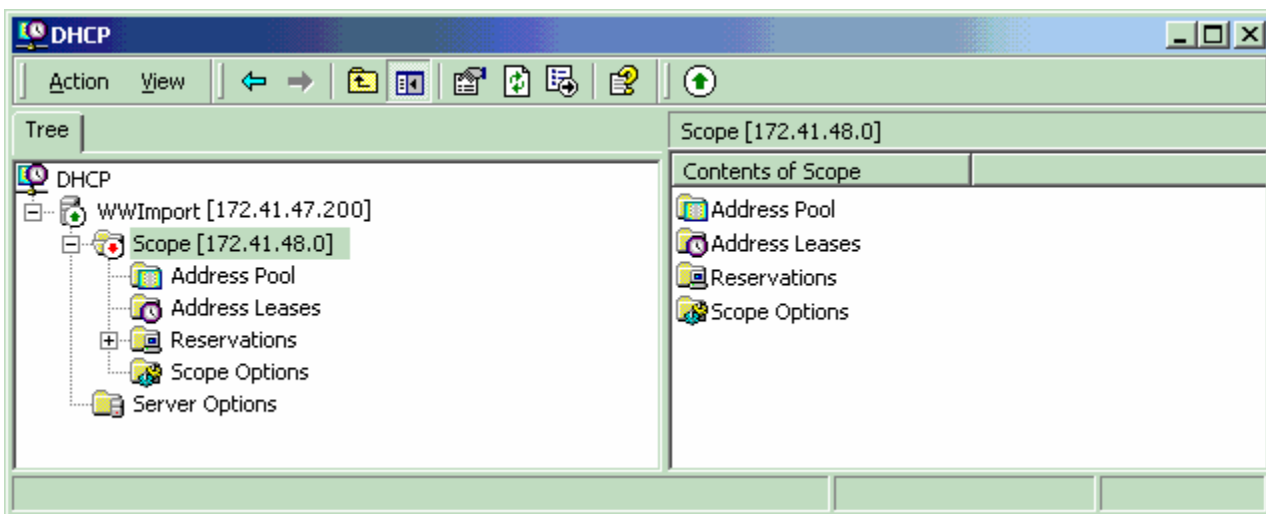
Scope 172.41.48.0 has been configured with the range 172.41.48.1 to 172.41.48.255 with a 20-bit mask.

Users inform that you cannot access information on any computer on the network. What should you do to correct the problem? (Choose Two)

    A. Activate the scope.
    B. Authorize the DHCP server.
    C. Increase the lease duration.
    D. Change the end IP address to 172.41.52.255
    E. Recreate the scope that uses the subnet mask of 255.255.224.0
    F. Recreate the scope that uses the subnet mask of 255.255.248.0
    G. Add reservations for each client computer.

Answer: A, F
Explanation:

A: In this scenario the client computers cannot access network resources. The problem is related to the DHCP scope. By examining the exhibit we see that the scope is not activated; there is a red marker on it. The scope has to be activated.

F: Changing the subnet mask from 20 bits to 21 bits will do no harm. It would decrease the number of hosts from 4096 to 2048. The scenario only mentions 60 client computers.

Incorrect Answers:

B: By examining the exhibit we see that the DHCP Server; there is a green marker on it. This indicates that the DHCP server is running. An unauthorized DHCP is not allowed to run, so the DHCP is already authorized.

C: Increasing lease duration is not necessary but it would not do any greater harm.

D: Changing the scope by changing the end IP address to 172.41.52.255 is not correct. The end IP address of the scope is correct, but the subnet mask must be changed.

E: A scope with a start address of 172.41.48.1 cannot have a subnet mask of 255.255.224.0, a 19 bit subnet mask. The subnet mask must be at least 20 bits.

G: Adding reservations for every client computer would be a daunting task, and nothing much would be achieved.

QUESTION NO: 128
You are the administrator of a Windows 2000 domain. The domain has six Windows 2000 Server computers, 400 Windows 2000 Professional computers and 250 Windows NT Workstation 4.0 computers.

Three of the Windows 2000 Server computers are the DHCP servers. The other three servers are DNS servers. The TCP/IP configuration of all the Windows 2000 Professional computers and Windows NT Workstation 4.0 computers is provided by DHCP servers. For fault tolerance all three DHCP servers are configured so that they have scopes for all the computers in the network.

You configure the DHCP servers to always register and update client computers information on the configured DNS servers.

To increase security, you configure the DNS zones on all DNS servers to only allow secure updates.

After you perform this configuration of the DNS zones, you discover that the client computer information in the DNS zones is no longer updated correctly when IP address changes occur for Windows 2000 Professional computers and Windows NT 4.0 Workstation computers.

You want IP address changes for client computer to appear correctly in DNS zones that only allow secure updates.
What should you do?

   A.   Add the computer accounts of the three DHCP servers to the DnsUpdateProxy global security group.
   B.   Configure the three DNS servers to use a time to live (TTL) interval on resource record that is shorter than the lease time used by the DHCP servers.

C.   Configure the three DHCP servers to enable updates for DNS client computers that do not support dynamic update.
D.   On the Windows 2000 Professional computers and Windows NT Workstation 4.0 computers, configure the DHCP client computers to not release the DHCP lease at shutdown.

Answer: A
Explanation: If a DHCP server performs a secure dynamic update on a name, the DHCP server becomes the owner of that name, and only that DHCP server can update the name. This problem occurs when you use multiple Windows 2000 DHCP servers on your network and also configure your zones to allow secure dynamic updates only.

The solution to this problem is to use Active Directory Users and Computers to add your DHCP server computers to the built-in DnsUpdateProxyGroup. This will permit all of your DHCP servers the secure rights to perform proxy updates for any of your DHCP clients.

Incorrect Answers:
B: Decreasing the TTL time at the four DNS servers would make increase replication between the DNS servers, but it would allow the DHCP servers to perform secure updates.
C: The DHCP servers are not able to perform secure updates.
D: This is a security problem, not a DHCP client configuration problem.

QUESTION NO: 129
You are the administrator of TestKing's network. To automate the configuration of TCP/IP client computers and network printers on your network you install and configure the DHCP server service on a Windows 2000 Server computer. You also create a scope that contains the range of valid IP addresses for your network.

To ensure that the TCP/IP network printers will always receive the same address, you create an exclusion range for the addresses in use by the printers. You also create addresses reservations for each printer.

You discover that none of the printers are receiving addresses from the DHCP server. The client computers report no configuration problems.
What should you do to correct the problem?

A.   Remove the address reservations for the printers.
B.   Remove the exclusion range for the addresses that are in use by the printers.
C.   Disable the address conflict detection feature of the DHCP server service.
D.   Enable the address conflict detection feature of the DHCP server service.

Answer: B

Explanation: In this scenario an exclusion range exists for the IP addresses used by the printers. This prevents the DHCP server from using any of these IP addresses. The exclusion range for the printers has to be removed.

Incorrect Answers:
A: The exclusion range, not the reservation, has to be removed.
C: Address conflict detection configuration concerns how the DCHP server detects address conflicts. It will not solve the problem with the excluded IP addresses.
D: Address conflict detection configuration concerns how the DCHP server detects address conflicts. It will not solve the problem with the excluded IP addresses.

QUESTION NO: 130
You are the administrator of TestKing's network. Your network is configured to use DHCP to automate the TCP/IP configuration of client computers on your network. The network consists of three subnets connected by a BOOTP-enabled router. All client computers are running Windows 2000 Professional. You have configured a DHCP server with a scope for each subnet as shown in the exhibit.
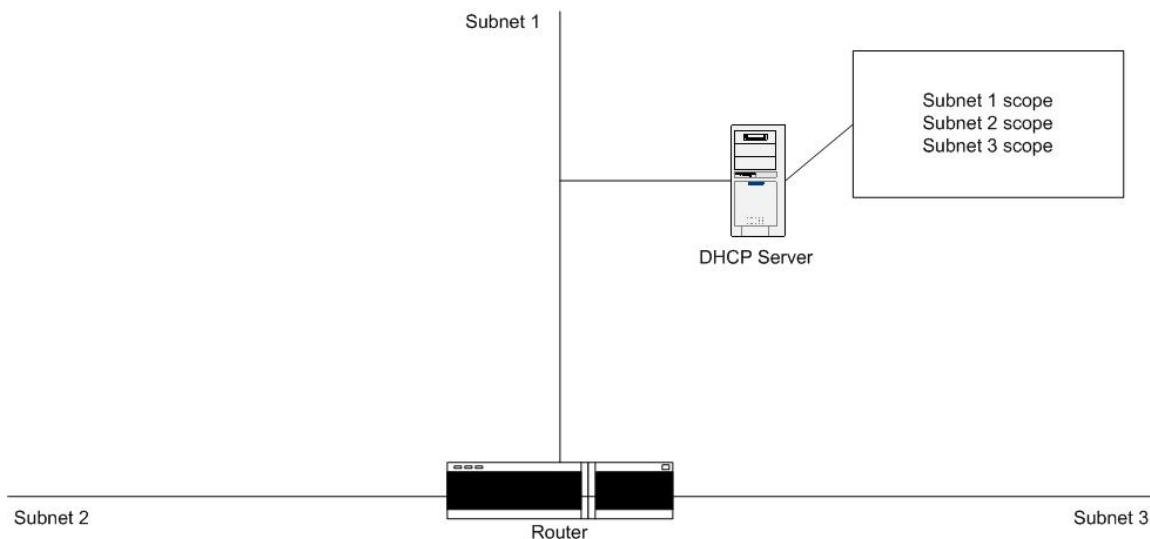
Users on subnet 2 and 3 report that they periodically cannot access the network resources. You discover that at times of high network usage, client computers on the remote subnets are being configured with addresses in the network address range of 169.254.0.0, which is not a valid address range on your network.

You want to ensure that all client computers receive addresses from DHCP and do not get configured with invalid addresses. What should you do?

   A.   Install a DHCP server on each remote subnet and configure a subnet-specific scope on each DHCP server.
   B.   Install a DHCP server on each remote subnet and configure identical scope on each DHCP server.

Leading the way in IT testing and certification tools, www.testking.com

C.   Install a DHCP relay agent on each remote subnet.
D.   Create an administrative template entry in Group Policy to enable automatic private IP addressing (APIPA) in the registry of each client computer.

Answer: A
Explanation: During times of high network usage, client computers on the remote subnets are configured with IP addresses in the 169.254.x.x range. This is the APIPA range, which is used to automatically configure clients when they are unable to receive IP configuration from the DHCP server. This apparently is a network bandwidth problem.
By installing a DHCP server locally on each remote subnet and configure it for that particular subnet, the clients would use the local DHCP server instead of the central DHCP server. This would reduce network traffic.

Incorrect Answers:
B: The DHCP servers should be configured with a local scope, not an identical scope on each of the DHCP servers. This will ensure that clients use their local DHCP server.
C: The remote clients are able to use the central DHCP, except during times of high network usage. Installing a DHCP Relay agent is not necessary and it would not reduce network traffic.
D: APIPA is enabled by default on Windows 2000 computers.

QUESTION NO: 131
You are the administrator of Windows 2000 network. The network consists of 15 Windows 2000 Server computer computers, 50 Windows 2000 Professional desktop computers and 200 Windows 2000 Professional portable computers. The portable computers are frequently utilized by users at locations that are not on the network.

The TCP/IP configuration of all the Windows 2000 Professional computers is provided by two DHCP servers on the network.

You want to configure different lease times for the desktop computers and portable computers. The desktop computers should use the default lease time. The portable computers should use a default lease time of four hours.

Which three actions should you take to achieve these goals? (Choose Three)

A.   On the portable computer, set the **DHCP class ID** setting to **Windows 2000 portable computer**.
B.   On the portable computer, set the **DHCP vendor class ID** setting to **Windows 2000 options**.
C.   On the portable computers, manually configure a DHCP lease time of four hours. Allow other TCP/IP parameters to be configured by the DHCP servers.
D.   On the DHCP servers, configure the scope so that it has an empty lease duration value.
E.   On the DHCP servers, define a new user class that has the ID specified on the portable computers.
F.   On the DHCP servers, configure the scope options to use a lease time of four hours for the portable computer user class.

G.   On the DHCP servers, create a superscope that has two scope ranges. Use one scope for portable computer so that it has a lease time of four hours and one scope for desktop computers so that it has a default lease time.

Answer: A, E, F
Explanation: User classes allow DHCP clients to differentiate themselves by specifying a User Class option. When available for client use, this option includes a user-determined class ID that can help to group clients of similar configuration needs within a scope, such as providing a shorter lease time for portable computers that move frequently or use remote access often. Typically a DHCP server will be used to distribute different options that are specific to the needs of clients. In this scenario, we need to: Set the DHCP class ID setting to 'Windows 2000 laptop computers'; on the DHCP servers, define a new user class that has the ID specified for the portable computers; and on the DHCP servers, configure the scope options to use a lease time of four hours for the portable computer user class. To set DHCP class ID information at a DHCP-enabled client computer running Windows 2000 we must open a command prompt and use the IPConfig command-line utility with the /setclass switch to set the DHCP class ID the client uses when obtaining its lease from the DHCP server. To configure a User Class Lease Time we must open the DHCP console, select the DHCP Server, open Scope, Right click Scope options, select Configure Options, select the Advanced ban, Select appropriate Vendor Class and User Class (=Windows2000LapTopComputers in this example), Select 051 Lease, and Enter lease time: 14400 (4 hours = 14400 seconds)

Incorrect Answers:
B: The vendor class is by vendors, not by users. The vendor class cannot be used to set a specific lease time for the portable computers.
C: Lease time cannot be configured at the clients.
D: The scope should be configured to use a lease time of four hours, not an empty lease time.
G: The idea of creating a scope for a specific type of computers is not practical. Instead we should differentiate the computers by using User Classes.

QUESTION NO: 132
You are the administrator of Windows 2000 domain named nwtraders.mstf. You install a DHCP server at one of TestKing's branch offices, you create a scope that has 60 IP addresses.

Users in the branch office inform that each time they restart their computers they receive the following error message "DHCP is unavailable." You investigate by using the DHCP audit log, which displays the following activity:

```
ID Date,Time,Description,IP Address,Host Name,MAC Address
00,12/05/99,01:19:56. ,Started,,
54,12/05/99,01:19:57,Authorization failed,,nwtraders.msft,
```

You want to ensure that your users no longer receive the DHCP errors. What should you do?

A.   Run the Jetpack command.
B.   Reconcile all scopes.
C.   Authorize the DHCP scope.
D.   Authorize the DHCP server.

Answer: D
Explanation: The audit file shows that the DHCP service tried to start but that the authorization failed. The reason is that the DHCP Server is not authorized in the Active Directory.

Authorization of DHCP servers in Windows 2000 is designed to avoid rogue DHCP server leasing illegally or incorrectly.
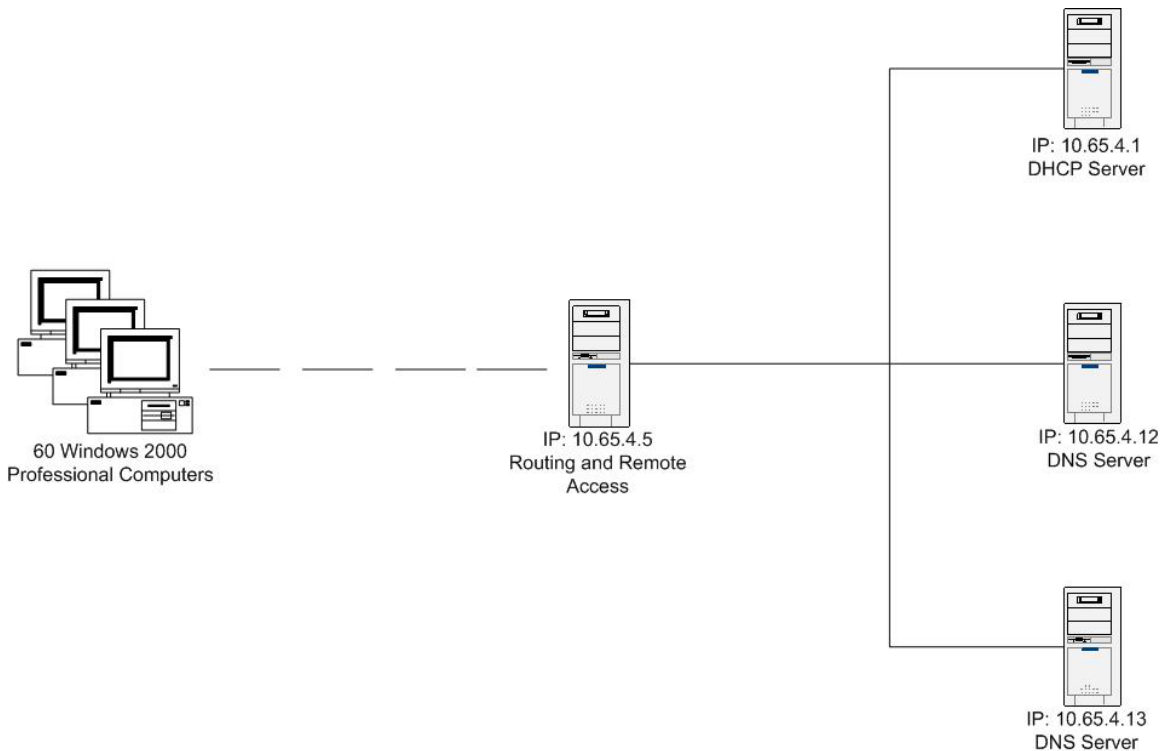
Incorrect Answers:
A: The jetpack command line is used to manage, for example compact, the WINS database file.
B: Scopes are reconsolided to renew the records of the DHCP database, it is not used to start the DHCP Server service.
C: DHCP scopes must be activated not authorized, before they can be used.

QUESTION NO: 133
You are the administrator of a Windows 2000 network. The network consists of a Windows 2000 based DHCP server, two Windows 2000 based DNS server, a Windows 2000 based routing and remote access server and 60 Windows 2000 Professional portable computers.

The network is configured as shown in the exhibit.

IP: 10.65.4.1
DHCP Server

IP: 10.65.4.5
Routing and Remote
Access

IP: 10.65.4.12
DNS Server

IP: 10.65.4.13
DNS Server

60 Windows 2000
Professional Computers

The DHCP server has a scope that has an IP address range of 10.65.4.20 through 10.65.4.80 with subnet mask 255.255.255.0.
You want the portable computers to use the DNS server that has an IP address of 10.65.4.12 when they dial in to the routing and remote access server. The routing and remote access server gathers IP addresses from the DHCP server for distribution to the portable computers when the portable computers dial in.
You configure the DHCP scope so that it has an IP address of 10.65.4.12 for the DNS servers scope option.
When users dial into the network by using the portable computer, all portable computers receive the IP address of 10.65.4.13 for the DNS server.
How should you configure the network so that the portable computers will receive the IP address of 10.65.4.12 for the DNS server?

    A.   Configure the DHCP server to always register and update client computer information to contain the configured DNS server.
    B.   Configure the routing and remote access server to use the LAN interface to obtain DHCP, DNS and WINS addresses for dial-up client computers.
    C.   Configure the LAN interface of the routing and remote access server to not use an IP address for the DNS server.
    D.   Enable the DHCP relay agent on the internal interface of the routing and remote access server. Configure the DHCP relay agent to use 10.65.4.1 as the IP address of DHCP server.

Answer: D

In this scenario there are two DNS servers on the network. The scope of the DHCP server has been configured to include the DNS address of 10.65.4.12. But when a RAS client gets access to the network they are configured with the IP address of the other DNS Server, 10.65.4.13. This can be explained by the fact that the RAS clients are not configured by the DHCP server, instead the RRAS server supplies IP Configuration, specifically the RAS clients get the same DNS settings as the RRAS server. The DHCPINFORM messages from the DHCP server are unable to reach the RAS clients. By enabling the DHCP relay agent on the internal interface of the RRAS server and configure it to use the DHCP server with IP address 10.65.4.1, the DHCP Relay agent will relay DHCPINFORM messages to the RAS clients and they will receive proper IP configuration.

Incorrect Answers:
A: In this scenario the RAS clients are unable to reach the DHCP server. Furthermore, configuring the DHCP server to always register and update client computer information would help downlevel computer to register in DNS, but it will not help them getting the correct IP address of the DNS server; therefore reconfiguring the DHCP server will not solve the problem.
B: In this scenario the RAS clients most likely already get the DNS, WINS of the RRAS server LAN interface. But this is not the correct network configuration for the RAS clients. They must be able to get DHCPINFORM messages from the DHCP server instead.
C: The RRAS servers LAN interface must have a DNS configuration so that the RRAS server can use network resources. The RAS clients get their DNS settings from the RRAS server LAN interface DNS settings. If the DNS setting of the RRAS server LAN interface is set not to contain an IP address, the RAS clients DNS setting would also be set not to contain an IP address.

QUESTION NO: 134
You are the administrator of TestKing's network. The relevant portion of its configuration is shown in the exhibit. .
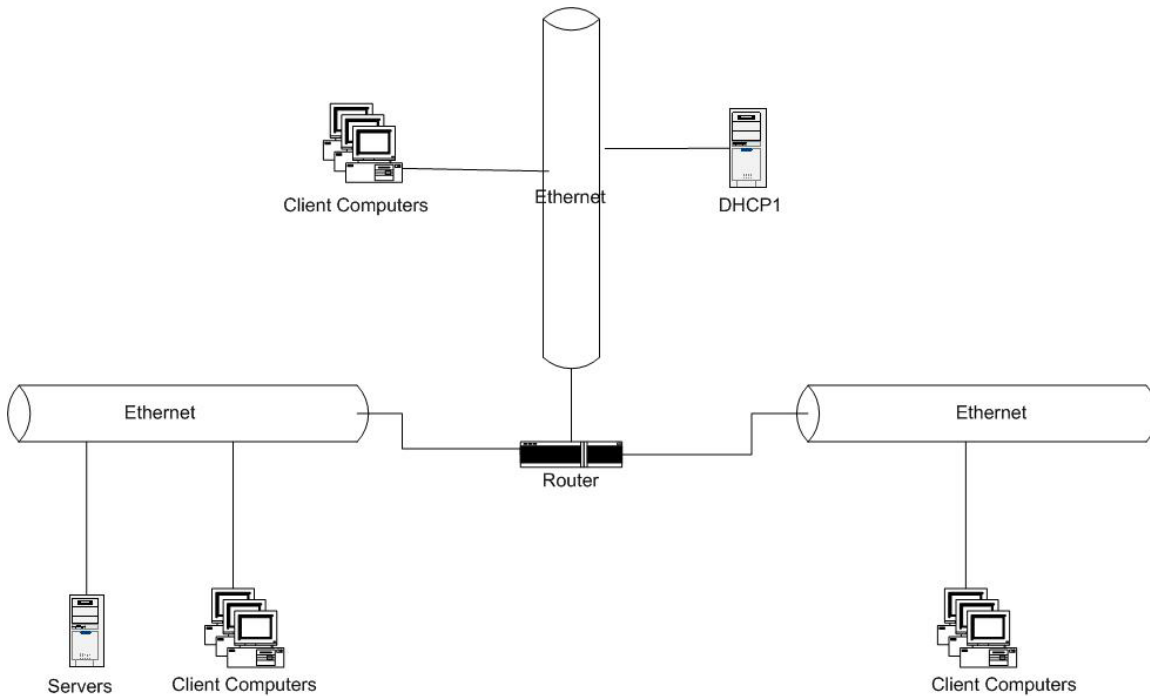
All client computers are DHCP clients. All servers have static IP addresses. The router is configured to forward BOOTP packets to DHCP1.

While you are performing hardware upgrades to DHCP1, you inadvertently delete the DHCP database file. You have no recent backup of this database.

You reconfigure the DHCP server with the correct scopes. Now you need to ensure that all computers on your network can obtain IP addresses, and that they experience no interruption in network connectivity.

What should you do?

    A.   Add IP address reservation for the servers
    B.   Run the **ipconfig/release** command and then the **ipconfig/renew** command on each client computer
    C.   Configure the DHCP server to delete address conflicts.
    D.   Add a scope option to enable dynamic DNS on client computers.

Answer: B
Explanation: By releasing and renewing the IP configuration of the clients, they would release their current IP address configuration and they would obtain new IP addresses from the DHCP server. This will ensure that obtain IP addresses from the correct scope.

Incorrect Answers:

Leading the way in IT testing and certification tools, www.testking.com

A: The servers use static IP addresses. These addresses should either be excluded from the scope or reserved. This would also not be our first step to solve this problem; we should renew the IP configuration on the clients.

C: We cannot configure a DHCP server to delete address conflicts. We can use address conflict detection to make the DHCP server check if an IP address is used, before it leases it to a client; but this is not the problem in this scenario.

D: Dynamic DNS is enabled by default on Windows 2000 computers.

QUESTION NO: 135
You are the administrator of TestKing's network, which currently consists of a single Token Ring network segment. You reconfigure the network to consist of two separate segments. The relevant portion of the resulting configuration is shown in the exhibit. .
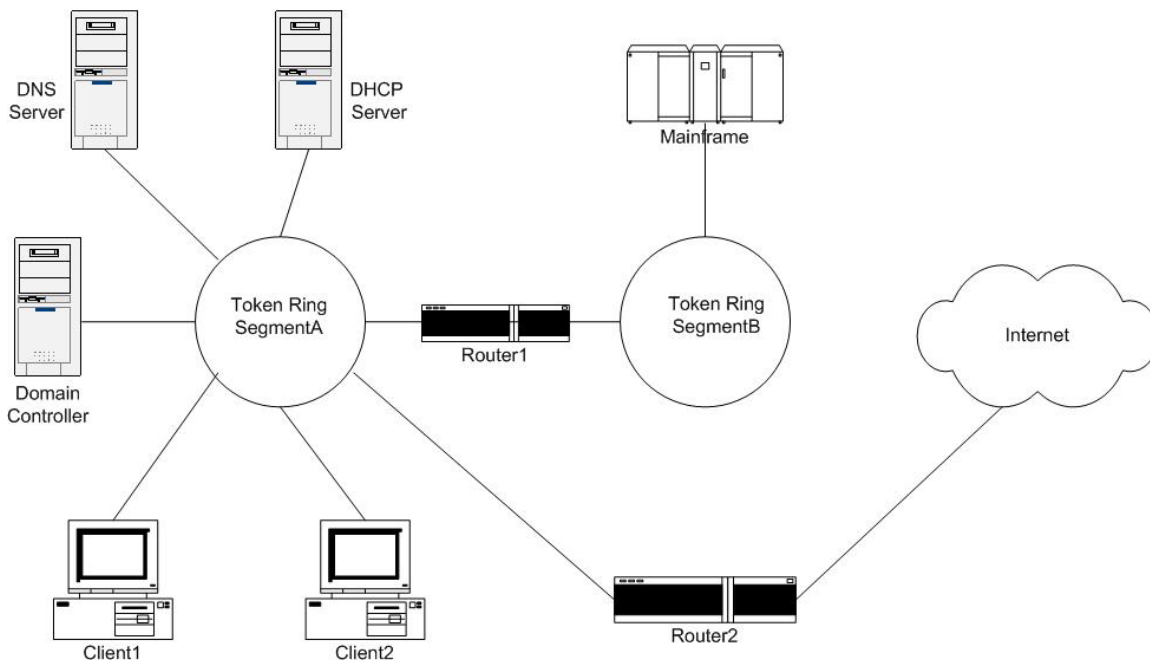
All client computers run Windows NT workstation 4.0, and all are DHCP clients. All client computers also run third-party TN3270 terminal emulation client software to connect to the main frame computer. All servers have static IP addresses.

Users now report that they cannot access Internet resource. They report no problems accessing resources on the mainframe computer.
From Client1, you ping a well-known Internet host. You receive the following error message: "Destination host unreachable."

You must ensure that client computer can access Internet resources without affecting connectivity for the mainframe computer. What should you do?

A.   Configure a DHCP global DNS option to be a DNS server on the Internet. Configure a Hosts file entry from the mainframe computer on each client computer.

B.   For DHCP clients on SegmentA, configure a DHCP scope Router option to be Router2. Configure a DHCP scope static Route option to specify the route to the mainframe computer.

C.   In the protocol binding properties for the client computers, move the DLC protocol below the TCP/IP protocol

D.   Disconnect Router2 from segment2 from SegmentA. Connect Router2 to SegmentB

Answer: B

Explanation: The clients are able to reach the mainframe on segmentB but they are unable to access Internet. The attempt to reach Internet using an IP address also failed (the ping command failed). This is not a DNS problem. In this scenario the clients on SegmentA are configured with a default gateway setting of Router 1 segmentA interface, since the clients are able to reach the mainframe. To solve this problem the clients must be able to be configured to use both routers. By creating a static route to the mainframe computer and by configuring the DHCP server scope Router option to Router2, the clients would be able to access both the mainframe and the Internet.

Incorrect Answers:

A: Configuring the DHCP scope DNS option to an external Internet DNS server would not provide Internet access since they clients still would be able to use router2. The clients must be configured to use router2, preferably by making router2 the default gateway.

C: Changing the binding order of the protocols would not get Internet access.

D: Connecting the Router 2 to SegmentB would not solve the Internet connectivity problem; on the contrary it would require even more configuration, since the clients on segmentA now would have to pass two routers before accessing Internet.

QUESTION NO: 136
You are the administrator of TestKing's network. All client computers run Windows 2000 Professional. All servers run either Windows 2000 Server, Windows NT server 4.0, or UNIX. All DNS servers run versions of BIND prior to 4.9.4.

You are planning a migration to an Active Directory domain structure. You install the DNS server service on several Windows 2000 member servers, choosing all default settings.

Now you need to migrate your existing DNS records to the new DNS servers, while maintaining your existing DNS servers as secondary DNS servers. Your solution must involve the fewest possible changes to your current network configuration.

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

A.   Upgrade all BIND versions to 8.2.2
B.   Disable fast zone transfers

C.   Copy and rename all zone files from the UNIX DNS servers to the systemroot\System32\DNS folder on the new DNS servers
D.   Initiate a zone transfer from the new DNS servers to the UNIX DNS servers
E.   Configure the new DNS servers with primary DNS zones. Configure the UNIX DNS servers as secondary zone servers.
F.   Configure the new DNS servers with Active Directory integrated zones. Configure the UNIX DNS servers as secondary zone servers.

Answer: B, D, E
Explanation: By default, all Windows-based DNS servers use a fast zone transfer format, which uses compression and can include multiple records per TCP message during a connected transfer. This format is also compatible with more recent Berkeley Internet Name Domain (BIND -based DNS servers that run versions 4.9.4 and later.
The DNS migration process in this scenario can be accomplished in three steps. First disable fast zone transfers on the Windows 2000 DNS servers. The reason for this is that DNS BIND 4.9.4 or later is required to support the fast zone transfer feature of Windows 2000 DNS. The fast zone transfer option is enabled by default in Windows 2000 DNS. Then initiate a zone transfer from the new DNS servers to the UNIX DNS servers. And configure the new DNS servers with primary DNS zones. Configure the UNIX DNS servers as secondary zone servers. To migrate from BIND servers using zone transfer we must install a DNS server on a Windows 2000 server computer. At the new server use the DNS console to add secondary zones for all of our existing zones hosted at the BIND-based DNS servers and configure the BIND servers as the master servers for each of the secondary zones you need to create. We must then initiate zone transfer at our Windows 2000 DNS servers to transfer the zones from the BIND servers. After completing the zone transfers, we must convert any of the secondary zones to primary zones that were obtained from primary zones at the BIND servers and for the other secondary zones that remain, we must update the master servers for those zones to use the new primary servers running Windows 2000 Server.

Incorrect Answers:
A: Upgrading all UNIX servers to BIND 8.2.2 would allow fast zone transfers and support for integration with Active Directory integrated zones. But it might not be possible and it would require more administrative effort than just disabling the fast zone transfers, by enabling BIND secondaries on the Windows 2000 DNS servers.
C: It is possible to migrate the UNIX DNS zones to Windows 2000 DNS, and this method of copying and renaming would work. Though it would require more administrative effort than simply initiate a zone transfer from a Windows 2000 DNS server.
F: The BIND DNS servers must be upgraded to version 8.1.2 or later to meet the DNS requirements for Active Directory support.

QUESTION NO: 137
You are the administrator o TestKing's network, which consists of a single Windows 2000 Domain. The network includes two domain controllers running Windows 2000 Server and two backup domain

controllers running Windows NT 4.0. Another Windows 2000 Server computer named VPN1 runs Routing and Remote access. All client computers run Windows 2000 Professional.

Employees who travel to customer sites use company-issued portable computers. These computers are configured for smart card support with company-issued certificates. Traveling employees dial in to VPN1 for network access.

You need to configure VPN1 to ensure that virtual private network (VPN) connections are as secure as possible.

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

    A.   Require Microsoft Point-to-Point Encryption (MPPE) for all dial-up users
    B.   Require L2TP/IPSec tunnel connections for all dial-up users
    C.   Require PPTP tunnel connections for all dial-up users
    D.   Require MS-CHAP v2 authentication for all dial-up users
    E.   Require EAP smart cards or certificates for authentication for all dial-up users.

Answer: C, E
Explanation: The portable computers are configured for smart card support with company-issued certificates. Only the Extensible Authentication Protocol (EAP) supports smart card authentication. In Windows 2000 there are two tunneling protocols: PPTP and L2TP/IPSec. L2TP supports tunnel authentication but Microsoft's PPTP implementation relies on the user's password as the basis for creating session keys for authentication and encryption. This reliance on user password makes the implementation, as weak as any user's password. This makes L2TP/IPSec more secure than PPTP. But you cannot use L2TP for dial up connections, so we will have to use PPTP.

Incorrect Answers:
A: Point-to-Point Encryption Protocol (MPPE) is only used for PPTP connections not L2TP connections.
B: L2TP cannot be used on dial-up connections.
D: Only EAP, not MS-CHAP V2, can be used for smart card authentication.

QUESTION NO: 138
You are the administrator of TestKing's network, which consists of a LAN with 2,000 computers on 15 subnets. Each subnet is a separate network segment.

You plan to create a test lab. Its environment will be similar to the environment of your existing company network. The test lab needs to provide at least 15 subnets. Three Windows 2000 Server computers are available for use as routers in the test lab.

You want to accomplish the following goals:

- **Provide the ability to conduct testing over multi-hop routes**
- **Provide the ability to reconfigure the test lab subnets for various testing scenarios with the least possible administrative effort.**
- **Minimize the network bandwidth consumed by routing protocol activity**
- **Enable all hosts in the text lab to be able to communicate with each other.**

You perform the following actions:

- **Enable routing and remote access and add RIP on all three Windows 2000 Server computers.**
- **Connect each Windows 2000 Server computer to the segments as shown in the exhibit. .**
- **Add each network interface on each router to RIP.**
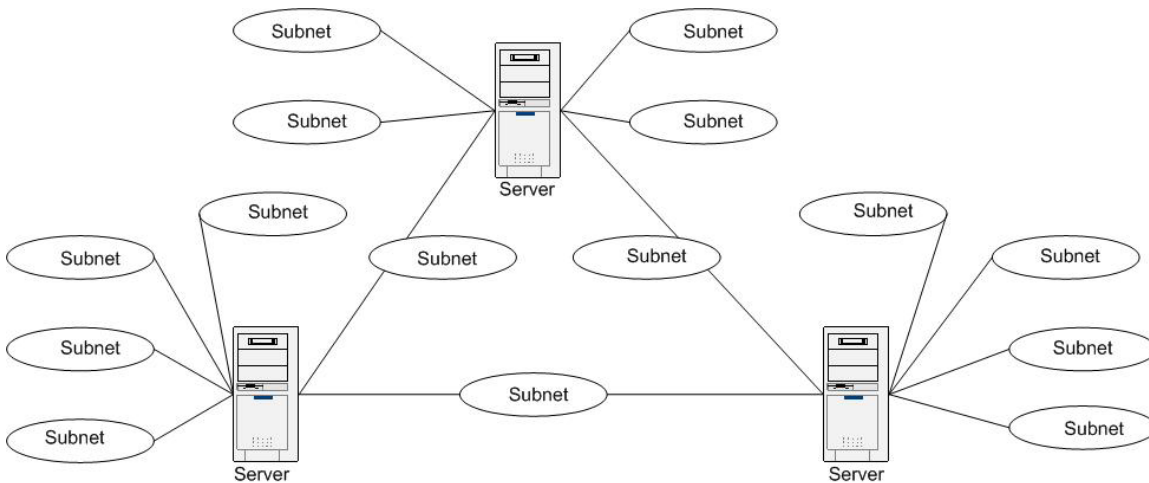
Which result or results do these actions produce? (Choose all that apply)

    A.   Testing can be conducted over multi-hop routes
    B.   The test lab subnets can be reconfigured for various testing scenarios with the least possible administrative effort
    C.   Network bandwidth consumed by routing protocol activity is minimized
    D.   All hosts in the test lab can communicate with each other.

Answer: A, B, D
Explanation:
A: RIP uses hop count as its metric. The maximum number of hops in a path is 15. This maximum will not be exceeded in this scenario.
B: RIP is self-configuring and does not need any administration when changing testing scenario.
D: RIP is self-configuring and by enabling routing and remote access and add RIP on all three Windows 2000 Server computers all hosts will be able to communicate with each other.
    The clients must be configured with a default gateway, which would be the IP address of a Routers LAN interface which connects to the client.

Incorrect Answers:
C: RIP uses regular broadcasts to keep its routing tables updated. This requires some network bandwidth. The OSPF routing protocol uses less bandwith, therefore the consumed network is not minimized.

QUESTION NO: 139
You are the administrator of TestKing's network. The relevant portion of its configuration is shown in the following diagram.
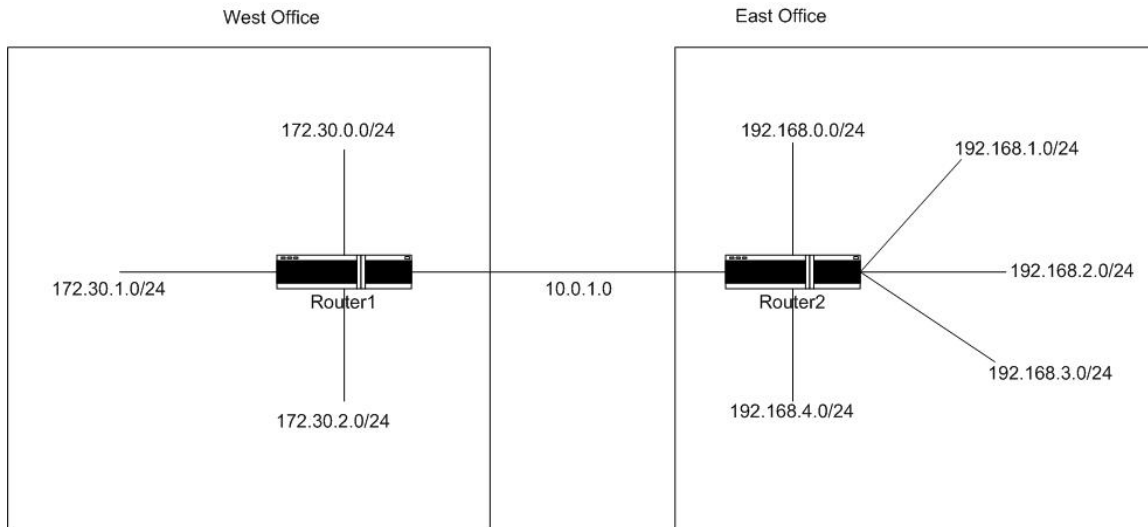
Projected growth in the West office will require five additional subnets during the next year. Projected growth in the East Office will require 10 additional subnets during the next year.

To reduce administrative complexity, you want to minimize the number of entries in the routing table for interoffice communication. You also want to provide for projected growth and conserve network address space.

Which subnet mask should you use for route summarization between the two offices?

To answer, click the select and place button, and then drag the correct subnet mask to the appropriate location.

Select and Place

Router1
Network Address   192.168.0.0
Subnet Mask   255.255.254.0

Possible Subnet Masks

255.255.224.0   255.255.252.0

255.255.240.0   255.255.254.0

255.255.248.0   255.255.255.0

Router2
Network Address   172.30.0.0
Subnet Mask   255.255.254.0
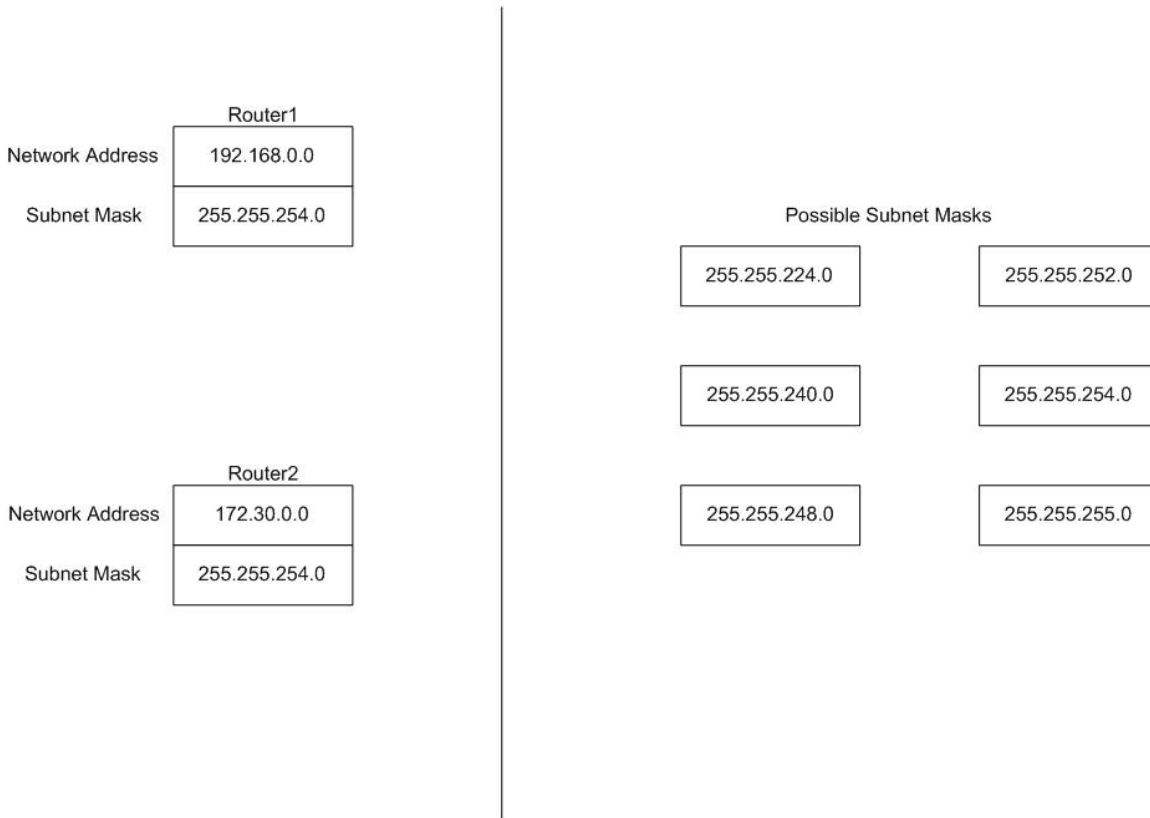
Answer: Router1: 255.255.240.0   Router2: 255.255.248.0
Explanation: Route summarization is used to summarize addresses of several prefixes into one prefix. This helps to control resource usage. Internetworks are divided into subnets.

In calculating the route summarization network mask we must consider minimizing the number of entries in the routing table for interoffice communication. This will be done by router summarization; providing for projected growth; and conserving network address space. The most restrictive working network mask must be used.

Router1
The router at the West office, Router1, contains routes to the East office. There are five subnets in the East Office,192.168.0.0, network. The projected growth is for an additional 10 subnet. A total of 15 subnets must be supported in the east network. These 15 subnets would be 192.168.0.0, 192.168.1.0, …., 192.168.14.0.
Subnets in binary:
11000000.10101000.00000000.00000000
11000000.10101000.00000001.00000000
…
…
11000000.10101000.00001110.00000000
As can be seen four additional bits will be needed for the host part. We will need a network mask of (binary):
11111111.11111111.11110000.00000000
In decimal: 255.255.240.0

Leading the way in IT testing and certification tools, www.testking.com

Router2

The router at the East office, Router2, contains routes to the West office. There are three subnets in the West Office ,172.30.0.0, network. The projected growth is for an additional 5 subnet. A total of 8 subnets must be supported in the east network. These 8 subnets would be 172.30.0.0, 172.30.1.0, …., 172.30.7.0.

Subnets in binary:

10101100.00011110.00000000.00000000

10101100.00011110.00000001.00000000

…

…

10101100.00011110.00000111.00000000

As can be seen three additional bits will be needed for the host part. We will need a network mask of (binary):

11111111.11111111.11111000.00000000

In decimal: 255.255.248.0

QUESTION NO: 140

You are the administrator if TestKing's network, which includes two Windows 2000 Server computers named Gate 1 and Apps2. The network also includes 50 client computers running Windows 2000 Professional.

Apps2 runs a custom client/server application that is used to store confidential information. Gate1 runs routing and remote access and provides connectivity to TestKing's Internet service provider by means of an ISDN connection. Gate1 also accesses information stored on Apps2. Client computers use Gate1 to access Internet resources.

You need to ensure that all communications with Apps2 are secure and encrypted. You apply the Secure Server IPSec policy to Apps2 and to Gate1, and you apply the client IPSec policy to all 50 client computers.

Users now report that they cannot access any Internet resources. On investigation, you discover that Gate1 connects to your ISP and then immediately drops the connection.

You must ensure that Gate1 can be used to access Internet resources. You must also ensure that communications with Apps2 remains encrypted. What should you do?

    A.   Remove the client IPSec policy from all 50 client computers
    B.   Remove the secure Server IPSec policy from Gate1 and assign the Server IPSec policy on Gate1
    C.   Remove the Secure Server IPSec policy from Gate1 and assign the Client IPSec policy on Gate1
    D.   Remove the Secure Server IPSec policy from Apps2 and assign the Server IPSec policy o Apps2.

Answer: B.

Explanation: The Secure Server (Require Security) security policy does not allow unsecured communications with clients. The Server (Request Security) policy causes the server to attempt to initiate secure communications for every session. If a client who is not IPSec-aware initiates a session, it will be allowed. The Client (Respond Only) policy allows communications in plaintext but will respond to IPSec requests and attempt to negotiate security. The problem in this scenario is that when Gate1 uses Secure Server (Require Security) security it will not accept the connection to Internet, since Internet is not IPSec enabled. By removing the secure Server IPSec policy from Gate1 and assign the Server IPSec policy on Gate1, Gate1 would accept Internet connections. All local connections would still be encrypted since Apps2 uses Secure Server and the client IPSec policy has been already been applied to the 50 client computers

Incorrect Answers:
A: By removing the client IPSec policy from all 50 client computers, Gate1 and Apps2 would no longer accept any connections to them.
C: If the Client (Respond Only) policy would be used on Gate1, the connections between Gate1 and the clients would be in plaintext.
D: Changing IPSec policy of Apps2 would not help. Gate1 would still require security and would not accept Internet connections.

QUESTION NO: 141
You are the network administrator for your company. For a test lab, you configure a single, dedicated network segment that consists of five servers and 40 client computers. The test lab must have connectivity to your production network. You are given an IP address range of 192.168.5.66 to 192.168.5.127 to use for the test lab.
You decide to configure one of the test lab servers as a Windows 2000 DHCP server. This server will automatically provide IP addressing information to the other computers in the test lab. You manually configure a static IP address and subnet mask of 192.168.5.10/24 on the new DHCP server.

You create a scope on the DHCP server for the 192.168.5.64/26 subnet. The scope includes an IP address range of 192.168.5.66 to 192.168.5.127. You successfully activate the scope on the DHCP server, but none of the DHCP clients can receive an IP address lease.

How should you correct this problem?

   A.   Edit the network address for the scope to be 192.168.5.0/24
   B.   Edit the network address for the scope to be 192.168.5.0/26
   C.   Edit the IP address and subnet mask of the DHCP server to be 192.168.5.65/26, and configure an exclusion for that IP address in the DHCP scope.
   D.   Edit the IP address and subnet mask of the DHCP server to be 192.168.5.66/26, and configure an exclusion for that IP address in the DHCP scope.

Answer: D

Explanation: In this scenario the subnet masks of the DHCP server and the scope are different. Therefore the DHCP would not be able to provide IP configuration for the clients.
By changing the network address for the scope to 192.168.5.0/24 the clients would to receive IP configuration information from the DHCP server.

Incorrect Answers:
A: By changing the network address for the scope to be 192.168.5.0/24, the scope would work, but it is not necessary to use large scope like that.
B: If the network address for the scope is changed to 192.168.5.0/26, the subnet masks would still differ.
C: You have been given the range 192.168.5.66 to 192.168.5.127 to use for the test lab. The IP address 192.168.5.65 is outside that range.

QUESTION NO: 142
You are the administrator of TestKing's network, which includes one Windows 2000 domain in native mode. Four servers on the network are available for remote users. All four are member servers running Windows NT server 4.0 and the routing and remote access service. Currently, remote access is administered individually by Active Directory user attributes.

You want to administer remote access by using centralized remote access policies. Which two courses of action should you perform? (Each correct answer presents part of the solution. Choose two)

   A.   Configure the four servers as RADIUS clients
   B.   Change the domain to mixed mode
   C.   Configure the four servers as domain controllers in their own Windows NT 4.0 domain. Create a one-way trust from the Windows NT 4.0 domain to the Windows 2000 domain.
   D.   On a Windows 2000 member server, configure the Internet Authentication service. Create a remote access policy on the IAS server
   E.   On a Windows 2000 member server, configure the Internet Authentication service. Create a remote access policy on a domain controller to administer all remote users.

Answer: A, D
Explanation: IAS is a Remote Authentication Dial-In User Service (RADIUS) server. RADIUS is a network protocol that enables remote authentication, authorization, and accounting of users who are connecting to a network access server (NAS). A network access server such as Windows Routing and Remote Access can be a RADIUS client or RADIUS server. IAS is used to centralize management of routing and remote access. To set up IAS we must install IAS on a Windows 2000 member server; create a remote access policy on the IAS server; and configure the four servers as RADIUS clients.

Incorrect Answers:
B: A native mode Windows 2000 domain cannot be changed to a mixed-mode domain. IAS and radius works on Windows NT.
C: With IAS the management is centralized. The Windows NT 4.0 servers are not domain controllers.

Leading the way in IT testing and certification tools, www.testking.com

E: With IAS the remote access policy should be centralized and created on the IAS server, not on any domain controller.

QUESTION NO: 143
You are the administrator of TestKing's network, which consists of a single segment. The network includes 100 client computers running Windows 2000 Professional and four servers running Windows 2000 Server. A server named AppSrv1 runs a client/server application that is used by every employee in the company.

Users report that network response times are very slow. When you examine the client/server application, you discover that it is transmitting large amounts of data to one client computer in the network. The application dos not indicate which computer is receiving the data.

You need to identify this computer. What should you do?

    A.   Run performance Monitor on your client computer. Create an alert that fires when network utilization exceeds 75 percent.
    B.   Run performance Monitor on AppSrv1. Create an alert that fires when network utilization exceeds 75 percent.
    C.   Install network monitor on your client computer by using the Windows 2000 server CD-ROM. Run Network Monitor and create a filter to capture packets sent to any client computer.
    D.   Install network monitor on your client computer by using the Windows 2000 server CD-ROM. Run Network Monitor and create a filter to capture packets containing the Ethernet address of AppSrv1.

Answer: D
Explanation: The filter should only capture traffic that is generated by the client/server application which is running on App1. The filter should only capture packets containing the Ethernet address of AppSrv1

Incorrect Answers:
A: Network monitor, not performance monitor (or the performance console), should be used to monitor network traffic.
B: Network monitor, not performance monitor (or the performance console), should be used to monitor network traffic.
C: The filter should be set capture traffic only from the AppSrv1, not for traffic send to any computer.

QUESTION NO: 144
You are the administrator of TestKing's network, which serves a single site with 150 users. The network includes eight servers running Windows 2000 server. One server hosts your internal web site. All servers have static IP addresses in the range from 10.1.1.2 through 10.1.1.10. All client computers run Windows 2000 Professional and are DHCP clients, using an address range of 10.1.1.11 through 10.1.1.200

You need to provide Internet access to internal users. To do so, you plan to use a pool of 100 IP addresses supplied by a contracted Internet service provider. Your solution must involve the least possible administrative effort.

What should you do? (Select two.)

    A.   Allow all client computers to use automatic Private IP addressing for IP address assignment. Configure all servers to use static IP addresses in the 192.168.0.0 subnet.

    B.   Install a server for network address translation. Add the IP address of the private interface of this server to the excluded range on your DHCP server. Change the IP address of the private interface for the network address translation protocol to 10.1.1.201.

    C.   Install a server for network address translation and enable the default DHCP allocator. Add the existing server addresses to the excluded range. Change the IP address of the private interface for the network Address Translation protocol to 10.1.1.201

    D.   Map internal addresses and port numbers of your servers to the pool of IP addresses and port numbers assigned by your Internet service provider.

Answer: B, D
Explanation:
B: We must an address translation scheme in this scenario. NAT would be sufficient. We must also make sure that DCHP is configured with proper exclusion range for the servers with static IP addresses. Furthermore, we should configure the internal interface of the NAT server with an appropriate static address.
D: Using NAT you can use several public IP addresses by mapping the internal addresses and port numbers to the pool of public IP addresses and port number used.

Incorrect Answers:
A: We must configure network address translation, either through NAT or through a proxy server.
C: We can't use both a DHCP server and the default DHCP allocator. If we want to use the DHCP allocator we must disable the DHCP service first.

QUESTION NO: 145
You are the administrator of TestKing's network. The network includes two UNIX DNS servers, three UNIX file servers, one Windows 2000 DHCP server, and 100 Windows 2000 Professional computers.
All Windows 2000 Professional computers are configured to obtain IP address assignments from the DHCP server. The DHCP server is configured to assign the addresses of both DNS servers to all clients for name resolution.

You want to replace your UNIX DNS servers with Windows 2000 DNS servers. You install the DNS server service on a new Windows 2000 Server computer. You configure this server to require secure dynamic updates. You update the DHCP scope to assign the address of the new DNS server to all client computers, and to stop issuing the addresses of the UNIX DNS servers.

Three days later, users report that they cannot access resources located on the UNIX file servers. You need to ensure that all users can access the resources on the UNIX file servers. What should you do?

A.   Install the DHCP relay agent in a Windows 2000 Professional computer located on the same subnet as the UNIX file servers

B.   Reconfigures the new DNS server so it does not require secure dynamic updates

C.   Create A (host) records on the new DNS server that point to the UNIX file servers.

D.   Create SRV (service) records that point to the UNIX file servers

E.   Create CNAME (canonical name) records that point to the UNIX file servers

Answer: C.

Explanation: The UNIX file servers are unreachable. They were unreachable before the UNIX DNS servers were replaced by the Windows 2000 DNS servers. The DHCP server is configured to assign the addresses of both DNS servers to all clients for name resolution. The Windows 2000 DNS servers is configured to require secure dynamic updates.

The Windows 2000 clients are able to dynamically register themselves in DNS, but the UNIX computers are not able to do that. A (host) records for UNIX file servers must manually be added on the Windows 2000 DNS server.

Incorrect Answers:

A: The DHCP relay agent cannot be installed on Windows 2000 Professional computers, only on Windows 2000 Server computers.

B: UNIX computers cannot register themselves dynamically in the DNS zone, even tough the "require secure dynamic" option is dropped at the DNS zone.

D: The UNIX file servers are not providing any network service in the domain, therefore it is not necessary to create SRV (service) records that point to the UNIX file servers.

E: CNAME (canonical name) records are used to create aliases of resources. An A (host) record for the UNIX file servers does not exist in the DNS server zone. Making a CNAME record with A (host) record would need work.

QUESTION NO: 146
You are the administrator of TestKing's network. Your DMZ network includes a DHCP server that provides IP addressing information to remote users. The relevant portion of the DMZ is configured as shown in the exhibit. .
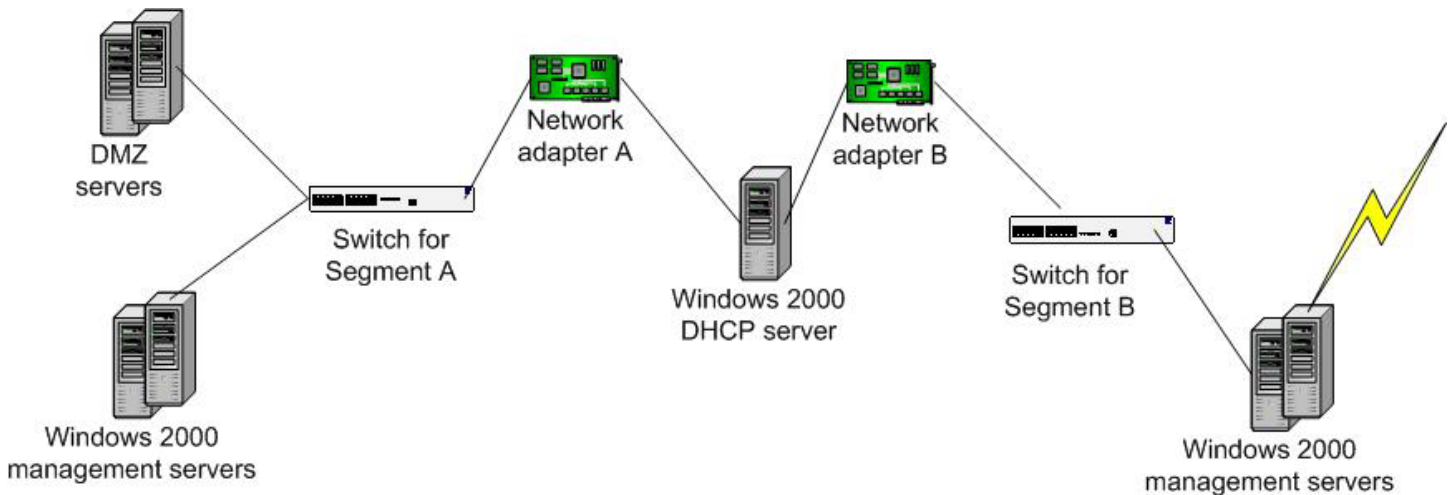
Every five minutes, the management servers collect performance and security log information from all servers on segment A.

You need to ensure that the DHCP server cannot issue IP addressing information to any DHCP clients on segment A. Your solution must be effective even if a valid scope for that segment is created on the DHCP server.
What should you do?

A. Disable the DHCP service binding to network adapter A
B. Disable TCP/IP binding to network adapter A
C. Disable NetBIOS over TCP/IP binding to network adapter A
D. Disable the client for Microsoft Networks on network adapter A

Answer: A.
Explanation: By disabling the binding of the service on an interface, we achieve a more efficient way of disabling DHCP response to clients, rather than completely removing TCP/IP which might result in a total loss of connectivity.

Note: To selectively set DHCP server bindings for network connections
1. Open DHCP
2. In the console tree, click the applicable DHCP server.
3. On the **Action** menu, click **Properties**.
4. Click the **Advanced** tab.
5. Click **Bindings**.
6. In the **Bindings** dialog box, for the list of **Connections and server bindings**, select or clear check boxes for any statically configured network connections that should be enabled or disabled for use at the applicable DHCP server.
7. Click **Apply**.

Incorrect Answers:

B: This proposed solution has a drawback. If we disable the TCP/IP protocol on the interface no TCP/IP traffic would occur on the interface. This might result in might result in a total loss of connectivity.

C: The "Disable NetBIOS over TCP/IP binding" is a WINS configuration and would not prevent DHCP leases on the interface.

D: Client for Microsoft Network is network service. Disabling it will not prevent DHCP issuing IP addressing information on segment A.

QUESTION NO: 147
You are the administrator of TestKing's network, which links your main office and one branch office. The network includes servers and client computers running Windows NT 4.0 in addition to servers and client computers running Windows 2000. You use both WINS and DNS for name resolution.

A computer named Remote1, located at the branch office, runs Windows NT server 4.0 and the routing and remote access service. Remote 1 is connected by means of a demand-dial connection to Corp1, which is located at the main office. Corp1 runs Windows 2000 Server and routing and remote access. Corp1 also functions as your WINS server and DNS server.

Regular analysis of the WINS Administrator statistics on Corp1 reveals that queries fail more than they success. Using Network Monitor, you discover failed queries from Remote1 to Corp1 for the name discover failed queries from Remote1 to Corp1 for the name JSPNRMPTGSBSSDIR. Further investigation reveals that the name is a broadcast from Remote1 for a non-registering service. Client computers can still connect to necessary resources. However, network traffic is increasing because of broadcast traffic and large numbers of log entries.

You want t stop the broadcast queries from Remote1. What should you do?

A. Create a static entry in the WINS database for JSPNRMPTGSBSSDIR. Map the entry to the IP addresses of the network adapters in Remote1.

B. Install WINS on Remote1, configured as a replication partner with Corp1

C. Add an entry to the LMHOSTS file on Remote1 for JSPNRMPTGSBSSDIR as the IP address of the local RRAS interface on Remote 1

D. Annually register JSPNRMPTGSBSSDIR on Corp1 by running the **nbstat –RR** command

Answer: C
Explanation: The name JSPNRMPTGSBSSDIR is announced regularly and is a normal occurrence from a Windows NT Server or Workstation computer running the Windows NT Remote Access Service (RAS). In this scenario the WINS server and DNS server are placed across a dial-up router on the network. This behavior causes unnecessary broadcast traffic across these interfaces. A trace at the main office from Network Monitor show queries for the name remote name JSPNRMPTGSBSSDIR.
Microsoft gives two possible solutions:
A. Create an LMHOSTS file with the entry:
```
x.x.x.x JSPNRMPTGSBSSDIR #PRE
```

Leading the way in IT testing and certification tools, www.testking.com

where x.x.x.x is an IP address associated with the RAS server's network interface card.
This corresponds to alternative C above.

B. Create an A record for JSPNRMPTGSBSSDIR in the domain for which the DNS server is authoritative.
This is not option here.

Reference:
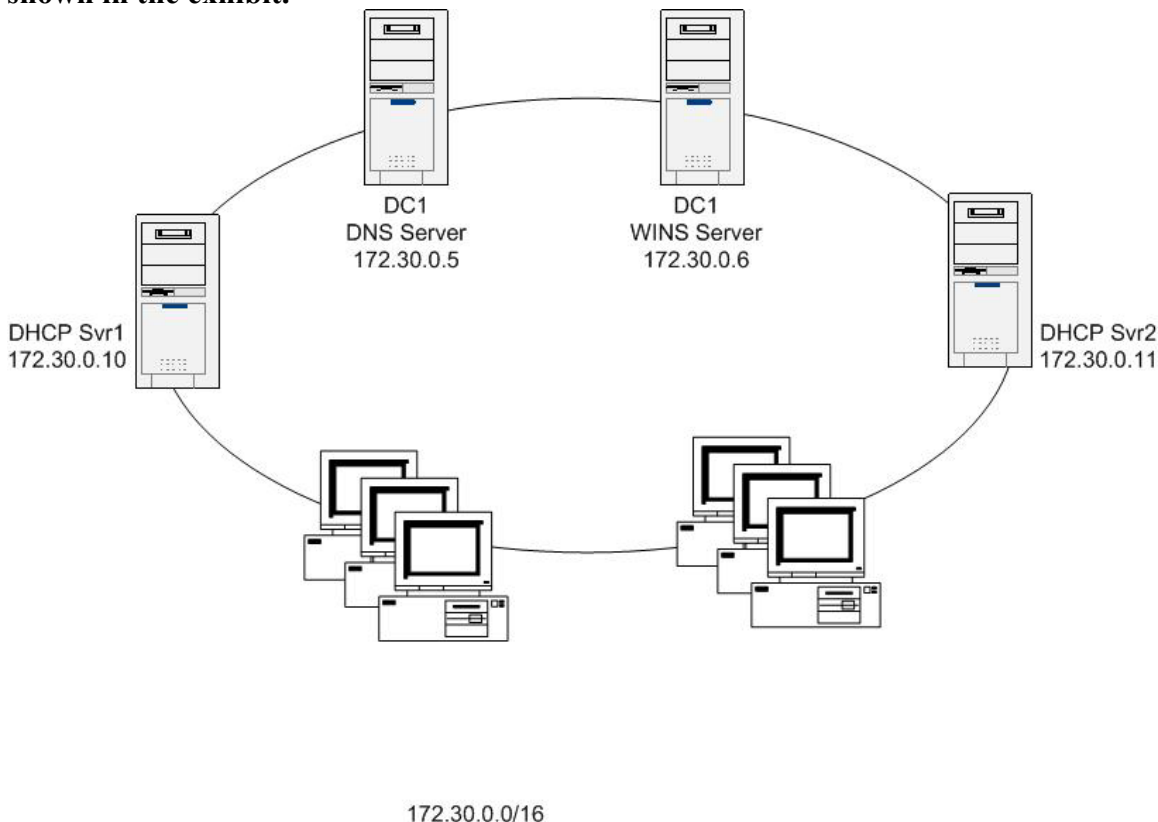RAS Service Broadcasts Name Query Every Two Minutes (Q150820)
WINS Statistics Show More Failures Than Successes (Q151475)

Incorrect Answers:
A, B, D: The problem, an remote Windows NT 4.0 RAS server broadcasting for the WINS name JSPNRMPTGSBSSDIR, is described in Q150820 and Q151475. The proposed solutions (A, B, D) are not given as possible solutions to the problem.

QUESTION NO: 148
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The network contains 5,000 client computers running Windows 2000 Professional. The network also contains two domain controllers named DC1 and DC2. The relevant portion of your network configuration is shown in the exhibit.

DC1
DNS Server
172.30.0.5

DC1
WINS Server
172.30.0.6

DHCP Svr1
172.30.0.10

DHCP Svr2
172.30.0.11

172.30.0.0/16

Leading the way in IT testing and certification tools, www.testking.com

You configure two DHCP servers with the scopes and scope options shown in the following table.

DHCP server	Scope	Scope options
DHCP-Srv1	172.30.0.100-172.30.100.254	006-172.30.0.5 044-172.30.0.6 046-0 x 8
DHCP-Srv2	172.30.0.100-172.30.100.254	006-172.30.0.5 044-172.30.0.6 046-0 x 8

Users now report that their computers often start very slowly. Users also report that they are often unable to access network resources. When you monitor the network, you discover that each DHCP server is issuing DHCPNACK messages to the other DHCP server and to requesting client computers

Which two actions should you perform to correct this problem? (Each correct answer presents part of the solution. Choose two)

    A.   Authorize DHCP-Svr1 in the domain
    B.   Authorize DHCP-Svr2 in the domain
    C.   Set an exclusion range of 172.30.50.0 to 172.30.100.254 on DHCP-Svr1
    D.   Set an exclusion range of 172.30.0.100 to 172.30.49.254 on DHCP-Svr2
    E.   Enable conflict detection on each DHCP server
    F.   Disable conflict detection on each DHCP server
    G.   Increase the lease duration on each DHCP server
    H.   Decrease the lease duration on each DHCP server

Answer: C, D
Explanation: The scopes of the DHCP servers are overlapping, which are a configuration error. We should make sure that you never configure multiple DHCP servers on the same LAN with overlapping scopes. If we do we might get the result described in this scenario.
Exclusion ranges could be used for redundancy. By excluding 50% of IP address at one DHCP server and excluding the other 50% of the other IP addresses there would be no overlapping scopes and DHCP would still work even if one of the DHCP servers fail.

Incorrect Answers:
A: Authorization of DHCP servers must be done to make them be able to run. But the DHCP servers are already running. Authorization is done to prevent rogue DHCP servers for register incorrect IP configuration.
B: The DHCP servers are already running, so they are already authorized.
E: Conflict detection might help somewhat, but the DHCP server have overlapping scopes and this quickly make the DHCP databases inconsistent.
F: Conflict detection is disabled by default. It will not help here.
G: In this scenario the overlapping scopes are the problem not the lease duration.

H: In this scenario the overlapping scopes are the problem not the lease duration.

QUESTION NO: 149
You are the network administrator for Trey Research. Your network contains a single Windows 2000 domain named treyresearch.com All servers and client computers on the network use static TCP/IP addresses.

You decide to implement DHCP on your network. You install Windows 2000 Server on a new computer named Tcpipsvr. You configure the server as a domain controller in a new domain named addressing.treyresearch.com , which is a child domain of TreyResearch.com

You install the DHCP service on Tcpipsvr. However, the service will not start. How should you correct this problem?

      A.   Configure the DHCP service to use a domain administrator account to log on to the domain
      B.   Demote Tcpipsvr to a stand-alone server. Add Tcpipsvr to TreyResearch.com
      C.   Log on to Tcpipsvr as an enterprise administrator and authorize Tcpipsvr
      D.   Log on to a TreyResearch.com domain controller as a domain administrator. Run the delegate control wizard on addressing treyresearch.com
      E.   Log on to addressing.treyreasearch.com as a domain administrator and authorize Tcpipsvr

Answer: C
Explanation: Windows 2000 DHCP servers in a Windows 2000 Domain are required to be authorized in the Active Directory before they are allowed to run. This feature is useful to prevent rogue servers from causing DHCP problems. The authorization must be done by a Enterprise Administrator.

Incorrect Answers:
A: The DHCP server service is run in the context of the localsystem. By running the DHCP service in the context of a domain administrator is unnecessary and could provide a security risk. It would make the DHCP server start.
B: Windows 2000 DHCP server must be authorized in the Active Directory before it can run. Demoting the server to stand-alone server would make it unable to authorize it.
D: The Delegation Of Control wizard steps you through the process of assigning permissions at the OU level. It would not to make the DHCP server to start.
E: The authorization must be done by a Enterprise Administrator, not by a domain Administrator.

QUESTION NO: 150
You are the administrator of TestKing's network, which consist of a single Windows 2000 domain. The relevant portion of its configuration is shown in the exhibit.
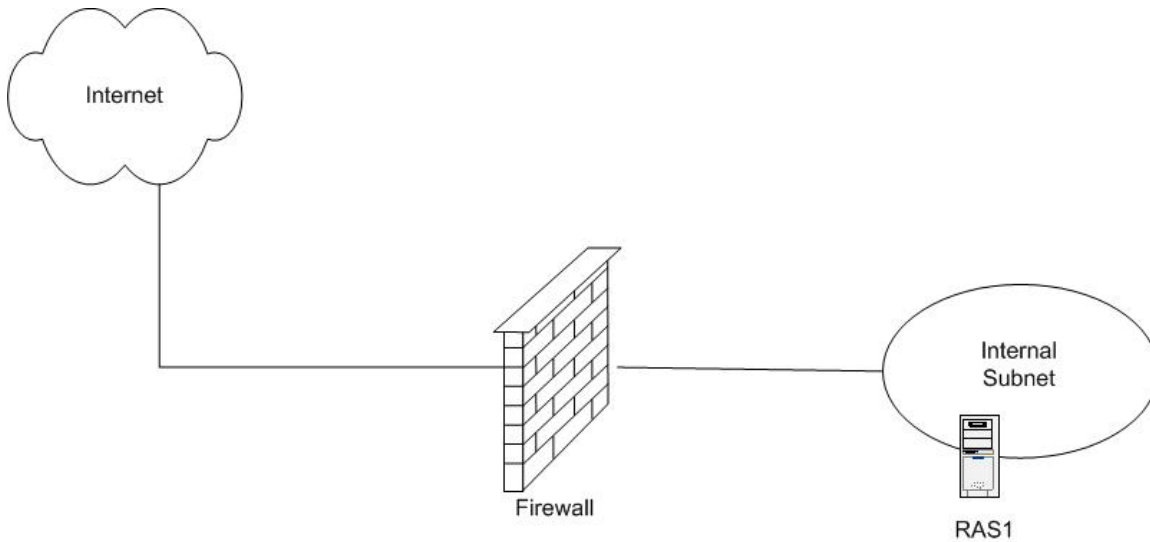
RAS1 is a Windows 2000 Server computer running routing and remote access. Your firewall is a hardware-based firewall solution that supports port filtering and General routing Encapsulation packet editing. All computers on your internal subnet use private IP addresses in the 10xxx range. The firewall provides network address translation for Internet access.

Company employees must be able to use the Internet to connect to your internal subnet. You need to ensure that the connections are as secure as possible.

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

A. Configure the client computers to dial in to RAS1 by using an L2TP virtual private network. Configure RAS1 to accept L2TP connections.
B. Configure the client computers to dial in to RAS1 by using a PPTP virtual private network. Configure RAS1 to accept PPTP connections.
C. Configure the firewall to route incoming traffic on the PPTP port to RAS1
D. Configure the firewall to route incoming traffic on the L2TP port to RAS1
E. Configure the firewall to edit the GRE call ID on incoming GRE packets
F. Install a server encryption certificate on RAS1

Answer: B, C, E
Explanation:

B: The firewall provides network address translation. This makes it impossible to use L2TP/IPSec since IPSEC changes the IP headers. We cannot use the L2TP protocol since it would not provide any security, which is a requirement. So the clients and the RAS server must be configured to use PPTP.

C: PPTP use port 1723 for maintenance traffic. Incoming traffic in this port should be routed to RAS1.

E: If we are using a PPTP tunnel, then we can place our VPN server behind the firewall if the firewall supports GRE packet editing, which is the case in this scenario. Unlike the TCP and IP protocols, which communicate on ports, the GRE protocol uses "call ID numbers" to establish sessions.

Reference: Technet: VPNs and Network Address Translators

Incorrect Answers:

A: L2TP/IPSEC cannot be used in connection with NAT.

D: There are no L2TP ports to be configured on the firewall. We must use PPTP not L2TP or L2TP/IPSec.

F: PPTP includes encrypted tunneling. Installing a server encryption certificate would not improve the encryption of the tunnel.

QUESTION NO: 151

You are the network administrator for the Baldwin Museum of Science. Your network includes a member server named Inet1, which is connected to the Internet. Inet1 runs Windows 2000 server.

Your institution sponsors joint research projects with Trey Research, whose main laboratory is located in another city. The Trey Research network includes a PPTP server named Trey3. You need to create a demand-dial router connection to this server.

You create a virtual private network demand-dial interface on Inet1. You use a domain account to configure the dial-out credentials, accepting default settings. However, you change the VPN server type from automatic to PPTP.

When you try to connect to Trey3, you receive an error message stating that access is denied. How should you correct this problem?

    A.   Change the tunnel type to L2TP/IPSec. Configure an IPSec policy on Inet1 and Trey3 for pre-shared key authentication.

    B.   Ensure that a new user account is created on Trey3. Change the dial-out credentials on Inet1 to use the new account

    C.   For the dial-out account on Inet1, obtain a certificate from a commercial certificate provider trusted by the Trey Research domain.

    D.   Ensure that the default remote access policy is removed from Trey3. On Inet1, change the VPN server type to automatic.

Answer: C

Explanation: Three authentication methods are available when forming a VPN: Kerberos 5, certificates and preshared secret key. The two most scalable methods, Kerberos and certificates, require Active Directory. Certificate authentication also requires access to a CA (certificate authority). If the two computers are in the same domain or in a trusted domain, you can use Kerberos authentication. By obtaining a certificate from a commercial certificate provider trusted by the Trey Research domain Inet1 would be able to authenticated by Trey3.

Incorrect Answers:
A: To use pre-shared key authentication L2TP/IPSec tunnel type must be used, the registry must be edited, and the IPSec Policy must configured for the pre-shared key. The registry has not been edited.
Note: To implement the Pre-shared Key authentication method for use with a L2TP/IPSec connection we must add the ProhibitIpSec registry value to both Windows 2000-based endpoint computers. We must then manually configure an IPSec policy before a L2TP/IPSec connection can be established between two Windows 2000-based computers.
B: Inet1 and Trey3 do not belong to the same domain. Therefore Kerberos authentication is not possible.
D: Removing that the default remote access policy from Trey3 would make it harder to get remote access.

QUESTION NO: 152
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. All employees use company-issued portable computers that run Windows 2000 Professional. These computers have computer accounts in the company's domain. These computers also contain a smart card reader, which is the only means of authentication for their users.

You need to provide secure access to network resources for users who work remotely. You enable Routing and Remote Access on a stand-alone Windows 2000 Server computer that is connected to the Internet. You also create ports for 25 PPTP virtual private network (VPN) connections. You verify that all VPN client connections are configured correctly.

To ensure security, you create a Routing and Remote Access policy and configure authentication as shown in the exhibit.

You need to enable all remote users to connect to the VPN server. You also need to ensure the highest possible level of authentication security.

What should you do?

A.   Join the VPN server to the domain and select **Smart Card or other Certificate** for the EAP method in the remote access policy.
B.   Configure 25 L2TP ports on the VPN server and remove the 25 PPTP ports
C.   Select the **Unencrypted Authentication (PAP, SPAP)** check box in the remote access policy
D.   Clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box in the remote access policy
E.   Clear the **Microsoft Encrypted Authentication version 2 (MS-CHAP v2)** check box in the remote access policy.

Answer: D
Explanation: We should clear the Microsoft encrypted Authentication (MS-CHAP) check box in the remote access policy as MS-CHAP uses a lower level of authentication than the MS-CHAP v2.

Incorrect Answers:

A: Only the company-issued portable computers has got smart card readers, and only these computers would be able to use EAP Smart Card or other Certificate. The users who work remotely and access the network through Internet cannot use EAP. They must use another protocol, preferably the MS-CHAP V2 protocol.

B: L2TP does not provide any encryption unless it is combined with IPSec. Therefore PPTP must be used.

C: PAP is unencrypted and shouldn't be an allowed authentication protocol.

E: Clear the MS-CHAP checkbox, not the MS-CHAP V2 checkbox. MS-CHAP V2 is more secure authentication protocol.

QUESTION NO: 153
You are the administrator of TestKing's network. The relevant portion of its configuration is shown in the following diagram.

All client computers run either Windows 2000 Professional or Windows 98. WinDNS1 runs Windows 2000 Server and the DNS server service. Router1 runs Windows 2000 Server and routing and remote access. Router1 also contains two network adapters. The first adapter connects to Subnet1 and is not configured with any TCP/IP filters. The second adapter connects to Subnet2 and is configured as shown in the exhibit.
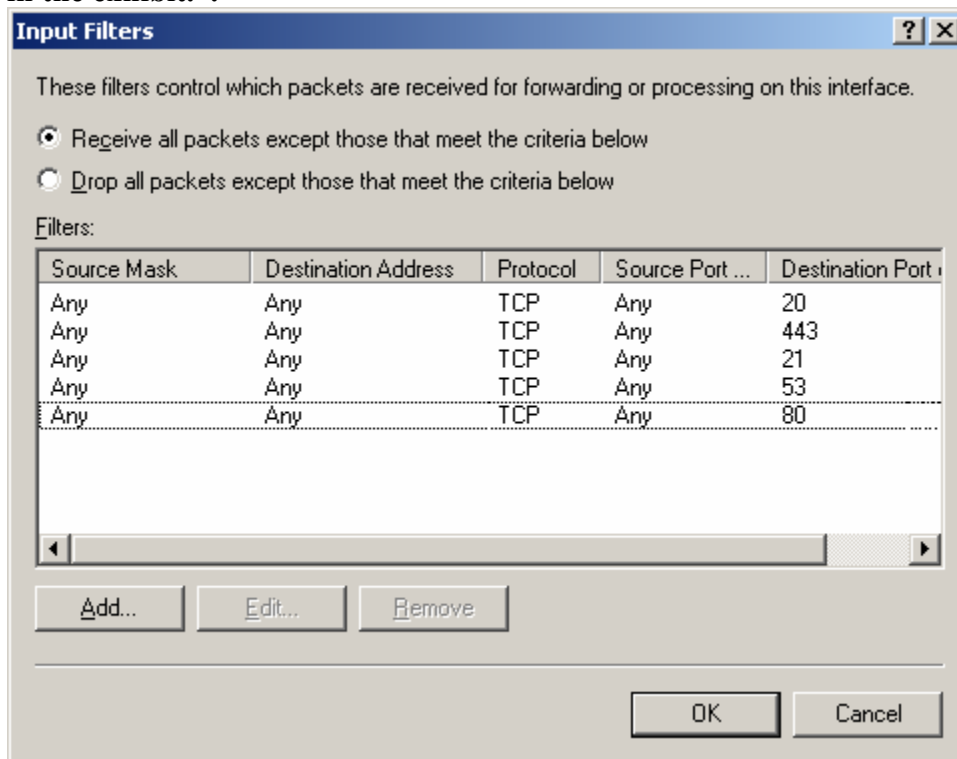
You want Router1 to enable users to access Web sites and FTP sites, while blocking other outgoing traffic. However, users report that they cannot access any Web sites or FTP sites.

Which action should you perform on Router 1 to correct this problem?

A.   On the network adapter for Subnet 2, delete the input filter for destination ports 80 and 443.
B.   In Routing and Remote access, move the input filters from the network adapter for Subnet2 to the network adapter for subnet1
C.   On the network adapter for Subnet2, change the input filters to drop all packets left unspecified rather than to receive all packets left unspecified.
D.   In routing and remote access, copy the input filters from the network adapter for subnet 2 to the output filters of the network adapters for subnet 1.

Answer: C
Explanation: By examining the exhibit we see that Subnet2 is set to "Receive all packets except those that meet the criterion below". And we see that the Destination ports of 20 (FTP), 21 (FTP), 53 (DNS), 80 (HTTP) and 443 (HTTPS). This means that no accesses to Web sites or FTP sites are allowed. By changing this setting to "Drop all packets except those that meet the criterion below" the only access provided would be access to FTP sites and Web Sites (and DNS server).

Incorrect Answers:
A: It is not necessary to delete the filter; it is applied incorrectly. It should drop, not receive, all packets except those that meets the criteria.
B: The input filter is correctly placed on network adapter on Subnet2, which connects to the Internet. It filters incoming network traffic.
           If the input filter were moved to network adapter for subnet, then the filter would be applied to all ingoing traffic to the local network. It would be almost work in the same way.
D: The input filter is correctly placed on network adapter on Subnet2, which connects to the Internet. It filters incoming network traffic. If the input filter were moved to the output filter for network adapter for subnet, then the filter would be applied to all outgoing traffic from the local network

QUESTION NO: 154
You are the administrator of TestKing's network, which initially consists of a single segment. You divide the network into four segments numbered 1 through 4. All four segments are connected by a single router. Each segment includes 50 client computers running Windows 2000 Professional and two servers running Windows 2000 Server.

An employee named Bruno uses a client computer located on segment2. He works with a custom client/server application that uses TCP/IP for communications. The application server is located on segment1.

Bruno's custom application intermittently returns error messages. You run network monitor on your client computer, which is located on segment 3. You perform a packet capture, but you cannot find any captured packets that were sent between Bruno's computer and the application server.

You need to examine the network traffic that is sent between Bruno's computer and the application server. What should you do?

A. Run Network Monitor on the application server and perform a packet capture
B. Create a Network Monitor trigger on your client computer and perform a packet capture
C. On your client computer, modify the Parsers.ini file and specify a parser for the client/server application. Perform a packet capture.
D. On your client computer, configure network Monitor to capture only packets that are sent from the Ethernet address of the application server. Perform a packet capture.

Answer: A
Explanation: Network Monitor monitors traffic only on the local network segment. To monitor remote traffic, you must use the version of Network Monitor that ships with Microsoft Systems Management Server (SMS) version 1.2 or 2.0. We are interested in traffic between Bruno's computer and the application server. By putting the Network Monitor on the application server and by filtering on Bruno's computer we would be able to capture all traffic between the two computers.'

Incorrect Answers:
B: Our computer is located on segment3, the application server is on segment1 and Bruno's computer is on segment2. Network Monitor monitors traffic only on the local network segment. We would not be able to monitor the traffic between Bruno's and the Application server from your computer.
C: We would not be able to monitor the traffic between Bruno's and the Application server from our computer.
D: We would not be able to monitor the traffic between Bruno's and the Application server from our computer.

QUESTION NO: 155
You are the administrator of TestKing's network, which includes a Windows 2000 Server computer named CorpllS. This server runs Internet Information Services and hosts a web application named WebApp. The application is used by internal users for company billing and invoicing.

TestKing's developers modify WebApp. Now the application allows downloads of your product catalog, encrypts communications between CorpllS and Web browsers, and accepts orders and credit card numbers from employees who access CorpllS from the Internet. You install the modified version of WebApp on CorpllS. You configure a TCP/IP packet filter to allow HTTP and FTP traffic to pass.

Users report that they can no longer access WebApp. When they try, they receive the following error message, "Web page requested is not available."
How should you correct this problem?

A. Assign the default server (Request security) IPSec policy on CorpllS.

B.   Create a custom IPSec policy for CorpllS that requests but does not require clients to use IPSec authentication.
C.   Configure a packet filter to allow TLS and SSL traffic to pass
D.   Configure the Web site properties on CorpllS to allow anonymous connections.


Answer: C
Explanation: In this scenario WebApp is used on the LAN by internal users. It is running smoothly. A modified version of WebApp is used by employees through the Internet. The modification includes encryption of communications between CotpIIS and Web browsers. This is either an authentication problem or an encryption problem. To clue to the problem is the error message "Web page requested is not available." This is not the error message an incorrect authentication attempt would produce. The available techniques to provide encryption through internet are to create a VPN with L2TP/IPSec or to use Secure Sockets Layer (SSL), also called HTTPS. In this scenario no VPN is used which leaves SSL. SSL (HTTPS) uses TCP port 443. The TCP/IP packet filer has been configured to only allow HTTP and FTP traffic to pass. By modifying the filter so that SSL traffic is allowed to pass, employees would be able to use the modified WebApp through Internet.

Incorrect Answers:
A: To be able to use IPSec a VPN connection must be established.
B: To be able to use IPSec a VPN connection must be established.
D: The error message indicates that this is not an authentication problem. It is an encryption problem.

QUESTION NO: 156
You are the network administrator for a test lab. The test lab network includes 10 network segments and five Windows 2000 computers configured as RIP routers. Periodically, the subnet configurations for the lab change to support varying testing requirements. A typical configuration is shown in the exhibit.
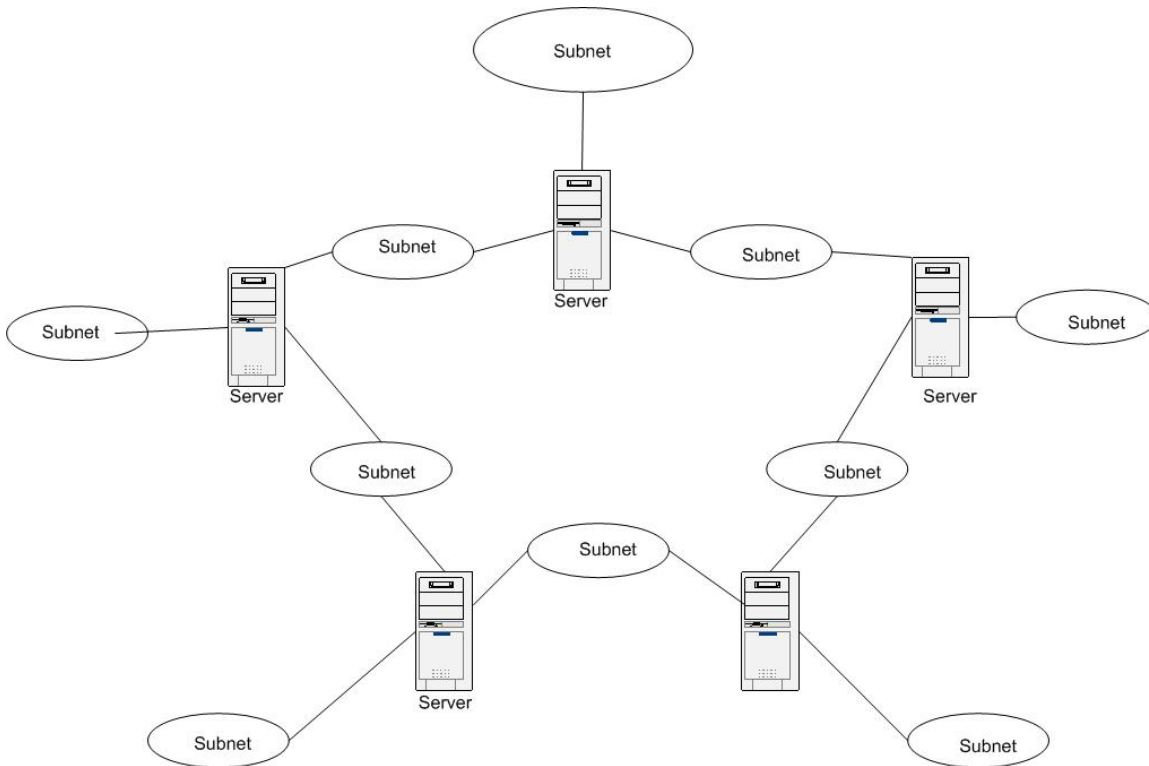
Sample network traces on several of the subnets show a significant amount of UDP port 520 broadcast traffic. You want to reduce the UDP broadcast traffic on the text lab network.

What should you do?

  A. Configure each router to accept announcements from listed routers only.
  B. Increase the **Periodic announcement interval** setting on the routers to 600 seconds.
  C. Increase the **Time before routes expire** setting on the routers to 3,600 seconds
  D. Configure the routers to use the auto-static update mode

Answer: B
Explanation: RIP uses regular broadcasts to keep its routing tables updated. These broadcasts use UDP port 520. These broadcasts are by scheduled for every 30 seconds. You can change this default setting by changing the **Periodic announcement interval** setting. By changing this setting to 600 seconds, the broadcasts would be scheduled for every 10 minutes, and broadcasts on UDP port 520 would decrease.

Incorrect Answers:
A: By configuring each router to accept announcements from listed routers only, you would decrease the work load of the routers, but it will not reduce RIP broadcasts.
C: The Time before routers expire setting has the default setting of 180 seconds. If the route is not updated in this time, it expires and is no longer a valid route. By increasing it to 3,600 seconds the routes would remain valid for a longer time, but it would not decrease the broadcasts on UDP port 520.

D: Auto-static updates are used for demand-dial interfaces not on other networks, instead Periodic update is used. Periodic update use the **Periodic announcement interval** setting, which is the setting that should be increased.

QUESTION NO: 157
You are the network administrator for Trey Research. Your network consists of a single segment with 150 client computers. Of these computers, 100 are desktop computers and 50 are portable computers. The portable computers are typically in use off-site. All client computers run Windows 2000 Professional and are DHCP clients.

The DHCP scope for the segment has the characteristics shown in the following table:

IP address range	Lease duration	Conflict detection attempts	Enable dynamic update of DNS records?
172.16.10.51 to 172.16.10.250	10 days	0	Yes

You disconnect the 100 desktop computers from the network and replace them with new hardware. When you connect the new computers to the segment, only 50 of them can communicate with other hosts on remote networks.

You need to enable all the new computers to communicate with remote networks. What should you do?

   A.   Disconnect the new computers from the network. Disable the automatic private IP addressing on the new computers, reconnect them to the network, and restart them.
   B.   Reconnect the old desktop computers to the network. On each new computer that cannot communicate with remote networks, run the **ipconfig/renew** command
   C.   Delete all the existing leases from the scope. Increase the setting for conflict detection attempts to **3.** On each computer that cannot communicate with remote networks, run the **ipconfig/renew** command.
   D.   Reduce the lease duration for the scope to one minute. After one minute has elapsed, reset the duration to eight days. Run the **ipconfig/renew** command on each computer on the network.

Answer: C
Explanation: The scope range contains 250 IP addresses. 50 are used by portable computers, 100 are used by the old desktops computers that has been removed. 50 are used by 50 new Desktops. 50 new Desktops do not have the correct IP configuration since the DHCP server has no IP address to lease them. The problem has occurred since the 100 removed computers still got leases in the DHCP scope. The lease time of the scope is 10 hours. By deleting the scope, increasing the setting for conflict detection attempts to **3,** and renewing all the IP leases, by IPCONFIG /renew, on the clients with no connectivity, all clients would receive proper IP configuration. By increasing the conflict detection attempts from the default 0 to 3 the DHCP server will

determine whether an IP address is already in use on the network before leasing or using the address. This is done by pinging the IP address, maximum 3 times, and see if there is any client responding to the ping. If no client responds the address is lease. If a client responds, that lease is added, and a new IP address is picked and tried.

Incorrect Answers:
A: Automatic private IP addressing (APIPA) is not the problem. It is the old leases on the DHCP scope.
B: The leases of the old desktops must be removed. Reconnecting the old desktops will not help.
D: By reducing the lease duration for the scope to one minute, new leases would only last for one minute. The old leases would still have a lease time of 10 hours.

QUESTION NO: 158
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain in native mode. The network includes 2,500 computers running Windows 2000 Professional and 30 computers running Windows 2000 Server. TCP/IP is the only network protocol in use. You install network monitor to provide performance baselines and to troubleshoot network traffic.

Most of TestKing's business occurs during regular business hours, which extend from 8:00A.M 8:00P.M, Monday through Friday. However, your customer service department operates 24 hours a day, seven days a week. Users in this department need to access a service database hosted on a computer named DBSvr1.

Customer service users who work from midnight until 8:00 A.M report access problems. Beginning immediately after midnight, these users cannot access DBSvr1 for short periods of time that occur at random intervals.

You examine the event logs for DBSvr1 but they contain no relevant error messages. You confirm that the database is functioning correctly. You decide to monitor network traffic during the period immediately before the first occurrence of the access problem each night.

You configure Network Monitor to begin a capture at the end of regular business hours. You also configure a client computer to send a message to the monitoring computer stating "No response," as soon as the access problem occurs.

Which three additional actions should you perform a Network Monitor? (Each correct answer present part of the solution. Choose three)

    A.   Filter frame size for headers only
    B.   Capture the entire datagram
    C.   Configure a trigger to Initialize when the buffer reaches 100 percent
    D.   Configure a trigger to initialize when the monitoring computer receives the message stating "No response"

E.   Configure a trigger to stop the trace when the monitoring computer receives the message stating "No response"
F.   Configure a trigger to stop the trace when the buffer reaches 100 percent.

Answer: B, C, E
Explanation: In this scenario we want to capture the network traffic which occurs immediately before the problem occurs. We do this by configuring to capture the entire diagram, we are only interested in small monitoring time Windows and we want as much information as possible from this time frame; starting the monitoring at midnight; reinitializing the monitoring every time the buffer reaches 100 percent to overwrite the capture buffer when it gets full; and stop the trace when we receive the message stating "No response". We stop the monitoring as soon as we know that the problem has occurred, and this way the correct data packets, the ones captured immediately before the problem occurred, will be in the capture buffer.

Incorrect Answers:
A: We are interested in all information we can get our hands on. We want to capture the whole frame.
D: The monitoring should end, not finish, when the monitoring computer receives the message stating "No response".
F: The traces should initialize (restart), not stop, when the buffer reaches 100 percent.

QUESTION NO: 159
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The network has a persistent connection to the Internet. The relevant portion of its configuration is shown in the exhibit.
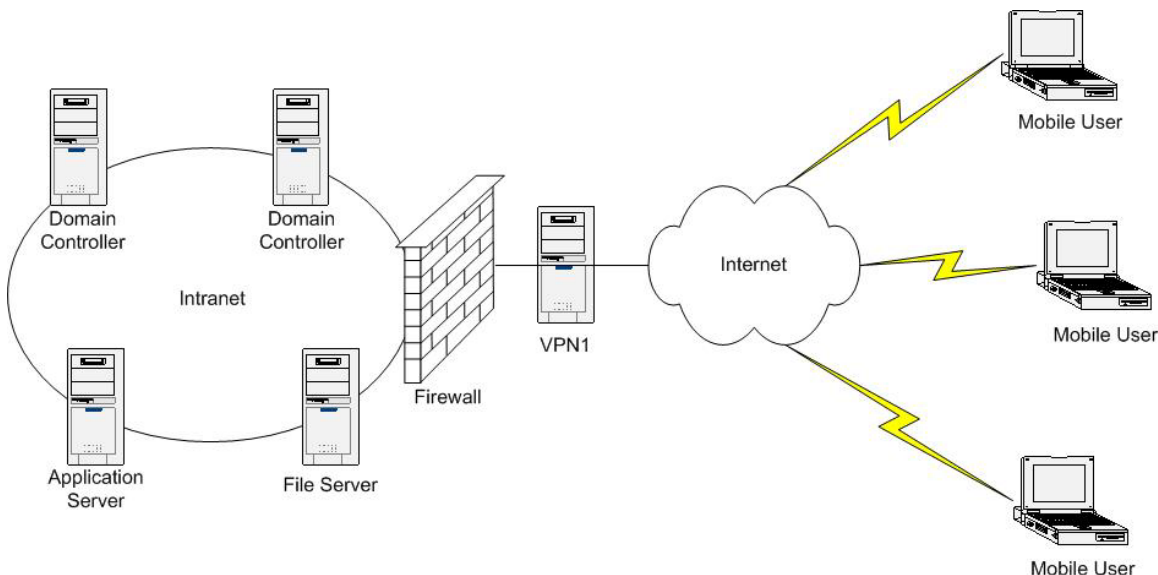
Your company employs mobile salespeople who use portable computers, which run either Windows 98 or Windows 2000 Professional. To enable these users to access internal resources, you place a virtual private

network server named VPN1 outside your firewall. VPN1 is a stand-alone Windows 2000 Server computer running routing and remote access. The firewall performs network address translation, and it is configured to allow inbound access from VPN1only.

You need to use the most secure VPN connection possible for each connection. You configure appropriate VPN ports on VPN1.

VPN1 must now be configured to allow only appropriate traffic through the firewall on the internal interface. Which output and input filters should you configure for the internal network adapter?

To answer click the select and place button, and the drag the correct filter configuration to the appropriate filter type. You might need to use some filter configurations more than once. Use the minimum number of necessary filters.

SELECT AND PLACE

	Destination: Firewall external address, TCP Port 1723	Source: Firewall external address, TCP Port 1723

Output Filters

	Destination: Firewall external address, UDP Port 500	Source: Firewall external address, UDP Port 500

	Destination: Firewall external address, TCP Port 1701	Source: Firewall external address, TCP Port 1701

	Destination: Firewall external address, IP Protocol ID 47	Source: Firewall external address, IP Protocol ID 47

Input Filters

	Destination: Firewall external address, IP Protocol ID 50	Source: Firewall external address, IP Protocol ID 50

	Destination: Firewall external address, any protocol	Source: Firewall external address, any protocol

	Destination: Internal subnet address, any protocol	Source: Internal subnet address, any protocol

Answer:
Output Filters
Source: Firewall external address, TCP port 1723
Source: Firewall external address, IP protocol ID 47

Input Filters

Destination: Firewall external address, TCP port 1723
Destination: Firewall external address, IP protocol ID 47

Explanation:
The firewall performs network address translations. The VPN must use PPTP, it cannot use L2TP/IPSec due the network address translation. Both IPSec and NAT changes the IP headers and they cannot both be used on a connection.

The VPN server is attached directly to the Internet and the firewall is between the VPN server and the intranet. In this configuration, the VPN server must be configured with packet filters that only allow VPN traffic in and out of its Internet interface.

PPTP use TCP port 1723 for tunnel maintenance traffic. For a filter to pass PPTP data it must allow IP protocol ID 47.

The source and destinations addresses that are usually used to allow VPN traffic is the IP address of the VPN server. In this case the firewall performs Network Address Translation so the Firewall external address is used instead.

Incorrect Answers:
PPTP does not use UDP port 500, it uses TCP port 1723.
PPTP does not use TCP port 1701, it uses TCP port1723.
PPTP does not use IP protocol ID 50, it uses IP protocol ID 47.
Only the PPTP port and the PPTP IP protocol ID traffic should be allowed, not any protocol.
The firewall provides Network Address translation. The Firewalls external IP address must be used, not the internal subnet address. There is no internal subnet address.

QUESTION NO: 160
You are the network administrator of the Adventure Works network. You plan to install a new Windows 2000 domain. The DNS zone for the new domain will be hosted on a server named BIND1, which runs UNIX and BIND.

You configure the adventureworks.com zone on BIND1 and enable dynamic updates. You configure a new Windows 2000 Server computer with the address of BIND1 and install the new server as your first domain controller.

The installation proceeds to completion without errors. However, when you try to join additional computers to the domain, you receive the following error message.

A domain controller for your domain could not be found.

You verify that the domain controller is running. You examine BIND1 and confirm that the records are being updated in the zone file. However, you discover that the master zone is not functioning. You also discover the following error message.

Master zone for "adventure-works.com" (IN) rejected due to errors.

You need to restore the functionality of the master zone on BIND1. What should you do?

    A.   Enable name checking on BIND1
    B.   Disable name checking on BIND1
    C.   Manually add SRV (service) records to the zone file on BIND1
    D.   Configure BIND1 to set authoritative AA bits on all responses.

Answer: C
Explanation: DNS name resolution is needed to locate Windows 2000 domain controllers. The Netlogon service uses DNS server support for the service (SRV) resource record to provide registration of domain controllers in your DNS domain namespace.
In this scenario clients and services are unable to the services in the domain. This is because the UNIX DNS server does not have any SRV (service) records in the DNS zone. These records have to be added manually.

Incorrect Answers:
A, B: There is no such thing as a "Name Checking" setting on a DNS Server.
D: Setting the authoritative AA bit setting would not help. It is a setting used for legacy clients. BIND normally caches negative responses, however, some very old servers and clients may have problems with this and generate errors. It's probably wise to upgrade those old clients and servers rather than turning this off.

QUESTION NO: 161
You are the administrator of TestKing's network. The relevant portion of its configuration is shown in the exhibit. . VPN1 and router1 run Windows 2000 Server and routing and remote access. Each server contains two network adapters named NIC1 and NIC2. Internal network users need to access both internal and external resources.

Leading the way in IT testing and certification tools, www.testking.com
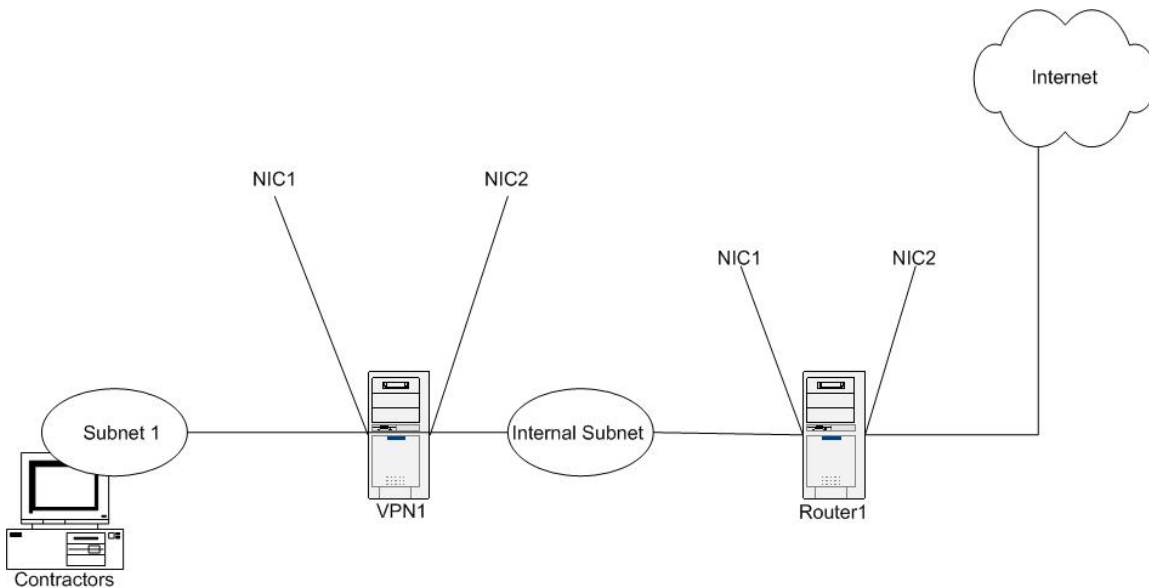
Subnet 1 is used by more than 10 contractors hired by your company. Their client computers run Windows 2000 Professional. Two contractors now need to access HTTP-based resources on your internal network. For security reasons, the contractors create a virtual private network connection that uses PPTP to access VPN1.

To reduce network traffic through VPN1, you want to prevent the contractors from accessing internet resources over the VPN tunnel. You decide to configure a TCP/IP input filter of one of your network adapters to drop HTTP traffic.

Which network adapter should you reconfigure?

    A.   NIC1 on Router1
    B.   NIC1 on VPN1
    C.   NIC2 on Router1
    D.   NIC2 on VPN1

Answer: B
Explanation: The contractors use a PPTP VPN connection to access VPN1. The contractors use HTTP resources on the Internal Subnet. They should not be allowed to access Internet resources.
By dropping all incoming HTTP traffic on NIC1 on VPN1, the contractors will not be able to access Internet, at least not with the HTTP protocol. They would still be able to access HTTP resources on the Internal Subnet, since this data is tunneled through NIC1 and will not be dropped.

Incorrect Answers:
A: Users on the Internal Subnet need to access HTTP based resources on the Internet. Dropping all incoming HTTP traffic on NIC1 on Router1 would make this impossible. HTTP traffic must be allowed to pass Router1.

Leading the way in IT testing and certification tools, www.testking.com

C: Dropping HTTP traffic on NIC2 on Router 1would stop all Internet HTTP traffic but it would also stop HTTP based resources on the Internal Network, and the contractors must be able to use these resources.
D: HTTP traffic must be allowed to pass VPN1 to allow the users on the Internal network to use HTTP resources on the Internet.

QUESTION NO: 162
You are the administrator of your company network. The relevant portion of its configuration is shown in the exhibit.
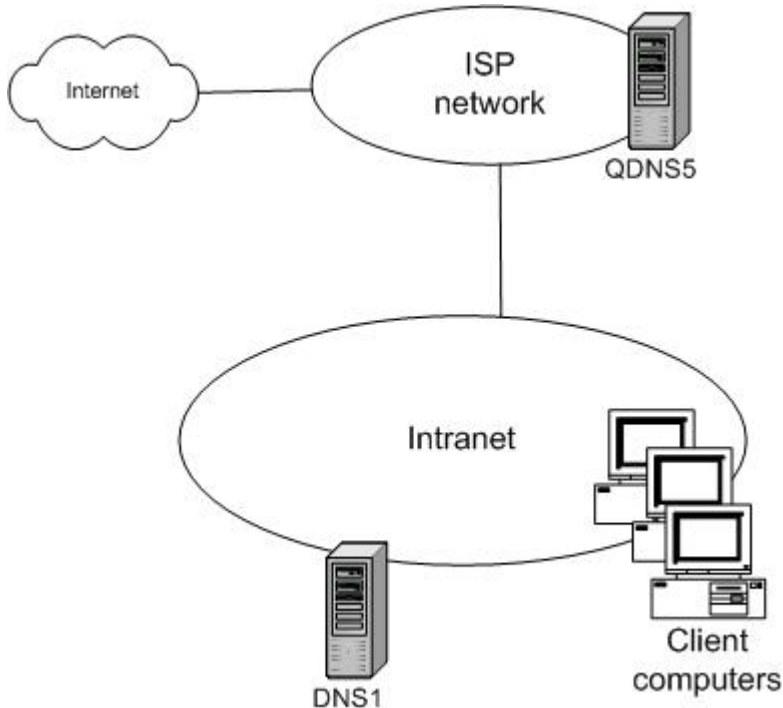
DNS1 is a Windows 2000 Server computer configured with a standard primary zone. QDNS5 is a UNIX server configured with a secondary DNS zone. QDNS5 accepts zone transfers from DNS1. The client computers on your network are configured to use DHCP to obtain IP addressing information. The DHCP server is configured to issue the IP addresses of DNS1 and QDNS5 to client computers for name resolution.

Users report that they sometimes cannot access any network resources by name. You discover that this problem occurs only when DNS1 has been taken offline for maintenance.

You need to ensure that users can resolve names from QDNS5 whenever DNS1 is unavailable. What should you do?

A.   Instruct your Internet service provider (ISP) to configure QDNS5 to Kerberos version 5 client software.
B.   Configure DNS Server service on DNS1 to allow BIND secondary servers.

C.   Instruct your Internet service provider (ISP) to upgrade the DNS server software on QDNS5 with a BIND 8.1 compatible implementation.
D.   Configure DNS1 so it does not require secure zone transfers.

Answer: B
Explanation: The zone transfers from DNS1 to QDNS5 is not working.
Bind secondaries determines whether to use fast transfer format when transferring a zone to DNS servers running legacy Berkeley Internet Name Domain (BIND) implementations. By default, all Windows-based DNS servers use a fast zone transfer format, which uses compression and can include multiple records per TCP message during a connected transfer. This format is also compatible with more recent BIND-based DNS servers that run versions 4.9.4 and later. In this scenario the ISP's DNS server does not appear to support this, and Bind secondaries needs to be enabled.

Incorrect Answers:
A: There is no need for Kerberos software on a DNS server.
C: We should first allow BIND secondary servers. This would allow replication traffic with UNIX BIND version 4.9.4 or later. There should be no need to upgrade QDNS5 to Bind 8.1.
D: The only secure zone transfers available are Active Directory integrated zone transfers, and they are not used here.

QUESTION NO: 163
You are designing TestKing's new WAN. The network consists of 50 Windows 2000 server computers, 2,500 Windows 2000 Professional computers, 2,000 Windows 98 computers and 50 UNIX servers. The Windows environment consists of a single Windows 2000 domain.

Users store data on both of their client computers and on the server computer using collaborative object between departments within the company.

The physical network consists of five subnets containing computer and a sixth subnet connecting to BOOTP routers as shown in the exhibit.
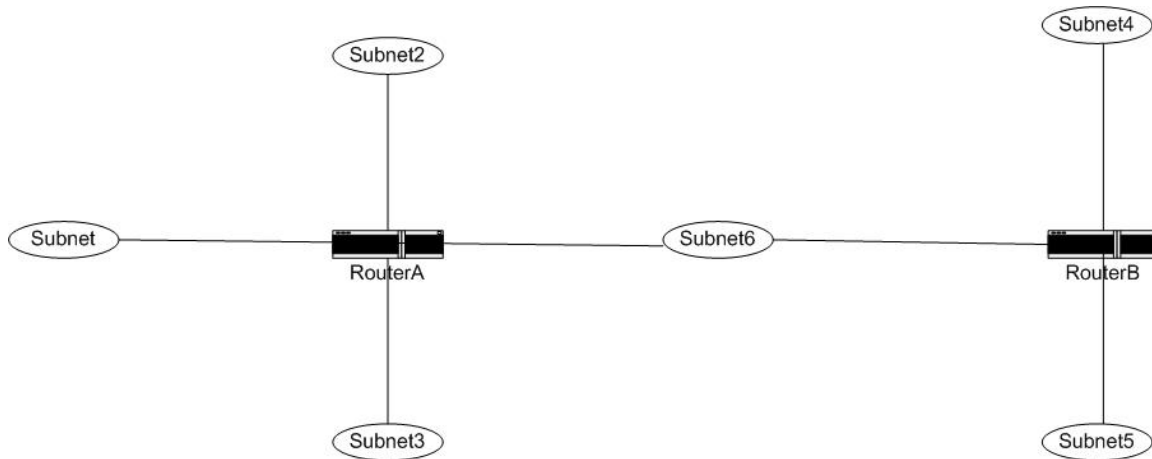
At present it is not necessary for connectivity within the network. You decide to use the reserve network IP address172.16.0.0. You are using DHCP to automatically configure client computers TCP/IP configurations. The server computers will have TCP/IP statically configured.
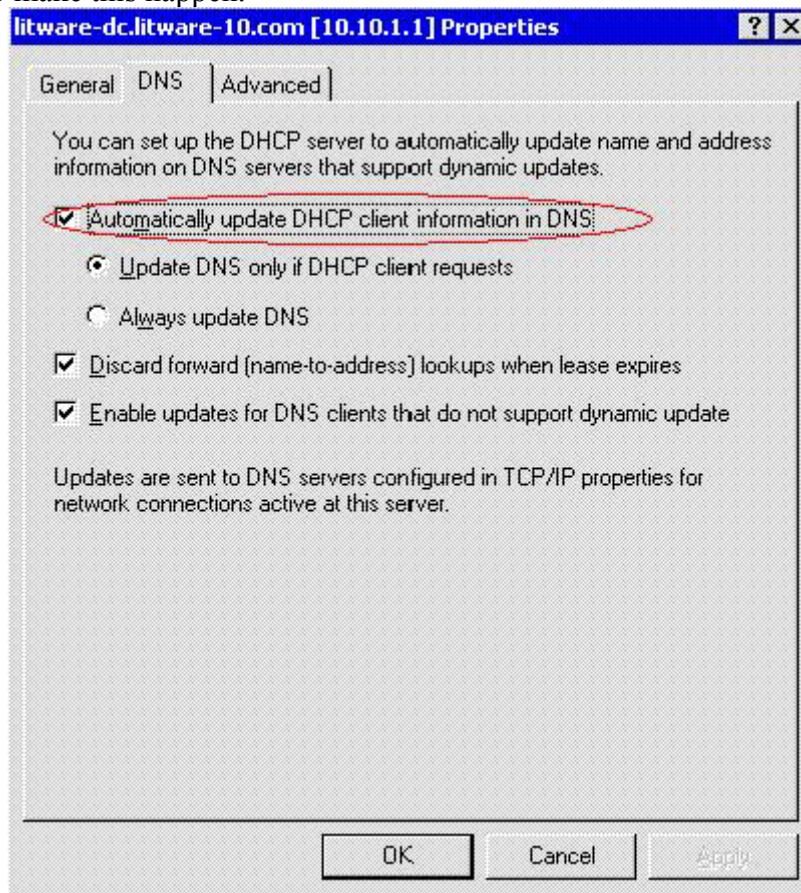
You want to accomplish the following goals:

- All users will be able to access resources located on all servers.
- All users will be able to access resources available on all client computers.
- Network traffic between the subnets will be minimized.
- The network will be able to accumulate growth of up to 100 percent over the next year with minimum reconfiguration of the physical infrastructure.

You take the following actions:

- Place all Windows 2000 server computers on subnet1.
- Place all UNIX servers on subnet2.
- Distribute the client computers evenly across subnet 3, subnet 4 and subnet5.
- Install the DHCP server service on one of the Windows 2000 server computer and configure a scope for each subnet including complete range of IP addresses default gateway and DNS settings.
- Install and configure DNS server service on one of the Windows 2000 server computer.
- Configure all Windows based computers to use DHCP.
- Subnet the network addresses placed by using the subnet mask 255.255.248.0.

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

A.   All users are able to access resources located on all servers.
B.   All users are able to access resources located on all client computers.
C.   Network traffic between subnets is minimized.
D.   The network is able to accommodate growth of up to 100% over the next year with the minimal reconfiguration of the physical infrastructure.

Answer: A
Explanation: The routers are BOOTP-enabled Therefore the DHCP IP configuration traffic will pass the routers and reach all clients. The IP configuration includes correct DNS and default gateway settings. This is done by using a different scope for each subnet. These clients will then be able to reach all servers, including the UNIX servers. All servers are configured for TCP/IP.

Incorrect Answers:

B: All clients have received proper IP configuration from the DHCP server. However, the Windows 98 clients would not be able to register themselves in the DNS zone. The default settings of the DHCP server is not to update DHCP client information in DNS (this is not required for Windows 2000 clients as they register themselves. The Windows 98 clients would not be accessible from the other computers. We would have to configure DHCP to **Automatically update DHCP client information in DNS** (see picture below) to make this happen.

litware-dc.litware-10.com [10.10.1.1] Properties

General | DNS | Advanced

You can set up the DHCP server to automatically update name and address information on DNS servers that support dynamic updates.

☑ Automatically update DHCP client information in DNS

    ◉ Update DNS only if DHCP client requests

    ○ Always update DNS

☑ Discard forward (name-to-address) lookups when lease expires

☑ Enable updates for DNS clients that do not support dynamic update

Updates are sent to DNS servers configured in TCP/IP properties for network connections active at this server.

OK | Cancel | Apply

C: To minimize network traffic you should install one DNS server and one DHCP server on each segment. This would decrease network bandwidth usage since DNS and DHCP traffic would be kept local on the subnet.

D: Currently there are 4600 (50+2,500+2,000+50) computers. And in a year it will double to 9200. Need 14 bits for hosts ($2^{13}=8192<9200<16384=2^{14}$). So subnet mask will be 18 bits:
Required subnet mask, binary: 11111111. 11111111.11000000.00000000

Required subnet mask, decimal: 255.255.196.0
The 21 bits subnet mask, 255.255.248.0, would only allow 2**11=2048 hosts.

QUESTION NO: 164
You are the administrator of a Windows 2000 network The network consists of a Windows 2000 server computer named ServerA and 15 Windows 2000 Professional computers. ServerA has a dial-up connection that connects to the Internet.

The 15 Windows 2000 Professional computers are configured to use automatic IP addresses (APIPA). There is no DHCP server on the network.

To allow the 15 Windows 2000 Professional computers to access the Internet through the dial-up connection of ServerA, you want to implement Internet Connection Sharing.

How should you configure Server A to accomplish this goal? (Choose all that apply)

  A.   Enable Internet Connection Sharing on the LAN interface of server A.
  B.   Enable Internet Connection Sharing on the dial-up connection of ServerA.
  C.   Configure ServerA to use a static IP address of 10.1.1.1 for the LAN interface.
  D.   Configure ServerA to use APIPA for the LAN interface.
  E.   Install and configure the DHCP server service on ServerA.

Answer: B
Explanation: Basically it is very easy to implement Internet Connection Sharing (ICS), it just have to be enabled on the Internet connection interface on the computer that should share its Internet connection. ICS provides many more features than just address translation. Microsoft has added many features to make the configuration of Internet connections as simple as possible. ICS can be fully configured and administered from the Routing and Remote Access Manager. For a simple home network, a Connection Sharing Wizard can also be launched from Control Panel Connections. The wizard does not allow configuration of any options but can get a home network up on the Internet in minutes. What simplifies the configuration is automatic addressing and automatic name resolution through the DHCP allocator, DNS proxy, and WINS proxy components. Each of these components provides a simplified configuration over the full version of DHCP, DNS, and WINS servers.

Incorrect Answers:
A: ICS should be enabled on the dial-up connection interface, not on the LAN interface.
C: When you enable Internet Connection Sharing, the network adapter connected to the home or small office network is given a new static IP address configuration. You should not assign a static IP address to it.
D: When you enable Internet Connection Sharing, the network adapter connected to the home or small office network is given a new static IP address configuration. You should not configure it for APIPA.
E: There is a mini-DHCP server, called DHCP allocator, included in ICS. In fact, ICS, would not work in a DHCP environment.

QUESTION NO: 165
You are the administrator of TestKing's network. Your company has a main office two branch offices and two small branch offices. The company network consists of one Windows 2000 domain. The main office and the two large branch offices are connected by a dedicated T1 lines as shown in the exhibit.
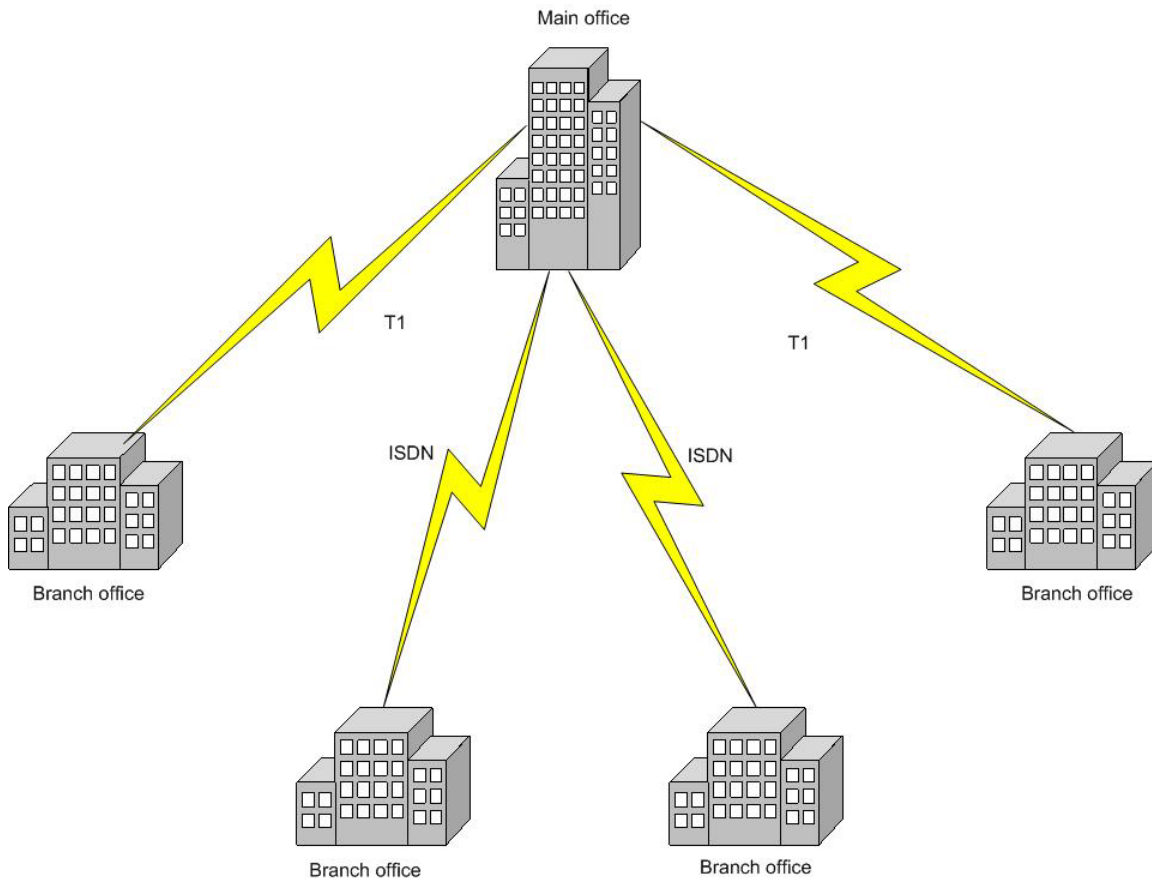
The two branch offices use 128 KBPS ISDN lines and routing and remote access over the internet to connect to the company's internal network. You are designing your DNS name resolution environment. You want to accomplish the following goals:

- **DNS name resolution traffic across the WAN links will be minimized.**
- **DNS replication traffic across the WAN links will be minimized.**
- **DNS replication traffic across the public WAN links will be secured.**
- **Name resolution performance for client computers will be optimized.**

You take the following actions:

- **Install the DNS server service on one domain controller at each office.**

Leading the way in IT testing and certification tools, www.testking.com

- **Create an active directory integrated zone on each DNS server at each office.**
- **Configure client computer to query their local DNS server.**
- **Configure the zones to allow dynamic updates.**

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

A.   DNS name resolution traffic across the WAN links is minimized.
B.   DNS replication traffic across the WAN links is minimized.
C.   DNS replication traffic across the public WAN links is secured.
D.   Name resolution performance for client computers is optimized.

Answer: A, B, C, D
Explanation:
A: A DNS server has been installed in each location and the clients have been configured use the local DNS
            server for name resolution. This minimizes DNS name resolution traffic across the WAN links.
B: Active Directory integrated zones replicates on a per-property basis, propagating only relevant changes.
            This is more efficient than full zone transfers. Additionally compression is used as well. This minimizes
            zone replication traffic.
C: Replication between standard and secondary DNS zones are unencrypted.. By creating an Active
            Directory integrated zone, DNS zone transfers will be included Active Directory replication. Active
            Directory replication uses secure channels which provides encryption.
D: A DNS server has been installed in each location and the clients have been configured use the local DNS
            server for name resolution. This minimizes slow DNS name resolution traffic across the WAN links and
            optimizes name resolution performance.

QUESTION NO: 166
**You are the administrator of a Windows 2000 network. Your network consists of two sides Denver and
Calgary. You have two DNS zones in your company.**

**The primary DNS server in the Denver is named ns1.contoso.com. The ns1.contoso.com server is
authoritative for the root zone contoso.com. The primary DNS server in Calgary is named
ns2.calgary.contoso.com. The ns2.Calgary.contoso.com server is authoritative for the delegated sub
domain calgary.contoso.com.**

**You examine the directory service log in Event Viewer on ns1.contoso.com and notice several knowledge
consistent checker (KCC) warnings. The warnings indicate that the KCC cannot establish a replication
link with directory partitions in the Calgary.**

**You decide to use nslookup to trouble shoot the problem. In the nslookup console you set the server to
ns1.contoso.com and the query type to all. In the nslookup console you enter the ls -d contoso.com
command. You receive a response as shown in the following graph.**

```
[ns1.contoso.com.]

contoso.com.            SOA    ns1.contoso.com.    administrator.contoso.com.
contoso.com.            A      192.168.1.200
ns1.contoso.com.        A      192.168.1.200
contoso.com.            NS     ns1.contoso.com.
ns2.calgary.contoso.com.    A      192.168.2.200
contoso.com.            NS     ns2.calgary.contoso.com.
```

You want to resolve the problem. What should you do?

    A.   Create the Host file on ns1.contoso.com server that creates the address for ns2.calgary.contoso.com.
    B.   Change the NS (name server) record that points to ns2.calgary.contoso.com to calgary.contoso.com. NS ns2.calgary.contoso.com.
    C.   On the ns1.contoso.com server, run the ns lookup-type=ns-norecurse contoso.com command.
    D.   On the ns1.contoso.com server, runs the nbtstat-a ns1.calgary.contoso.com command.

Answer: B
Explanation: In this scenario there are two domains: contoso.com (root domain) and calgary.contoso.com (subdomain). The DNS server ns1.contoso.com is authoritative for the root zone contoso.com. The ns2.calgary.contoso.com server is authoritative for calgary.contoso.com.
The KCC warnings indicate a replication problem. It cannot reach its replication partner in the calgary.contoso.com domain. The nslookup utility is then used to issue the command **ls -d contoso.com**
This lists all records for the contoso.com domain.
The NS (name server) records are:
contoso.com   NS ns1. contoso.com
contoso.com   NS ns2.calgary.contoso.com
The first record denotes that ns1.contoso.com is authoritative the contoso.com zone.
The 2nd record denotes that ns2.calgary.contoso.com is authoritative the contoso.com zone as well.
The second NS record is incorrect and should be replaced by:
calgary.contoso.com   NS ns2.calgary.contoso.com

Note: NS, name server, records.
The general format is <domain> NS <DNS server>
The name server (NS)resource record is used to notate which DNS servers are designated as authoritative for the zone. By listing a server in the NS RR, it becomes known to others as an authoritative server for the zone. This means that any server specified in the NS RR is to be considered an authoritative source by others, and is able to answer with certainty any queries made for names included in the zone.

Incorrect Answers:
A: There is already a A (host) record for ns2.calgary.contoso.com present. Adding another with a host file will not help.
C: We need to change a incorrect NS (name server) record. NSLOOKUP is command-line utility, which use reverse lookup queries to report back host names. It cannot be used to change records.
D: Nbstat is utility which is used to troubleshoot WINS problems. In this scenario we have DNS problem, not a WINS problem.

QUESTION NO: 167
You are the administrator of Windows 2000 network. The network consists of two Windows 2000 server computers named ServerA and ServerB and 180 Windows 2000 Professional computers on one segment.

ServerA has an IP address of 192.168.2.1. ServerA is a DHCP server. The TCP/IP configuration of all the Windows 2000 Professional computers is provided by the DHCP server. The range of IP addresses used at ServerA is 192.168.2.0/24. The lease time used is 15 days.

You want to change the IP address on the network from 192.168.2.0/24 to 10.17.8.0/24. Server B has an IP address of 10. 17. 8. 1. You install another DHCP server on the server B. the range of IP address used by ServerB is 10. 17. 8. 0/24. The lease time used is 15 days.

The network is shown in the following graph.
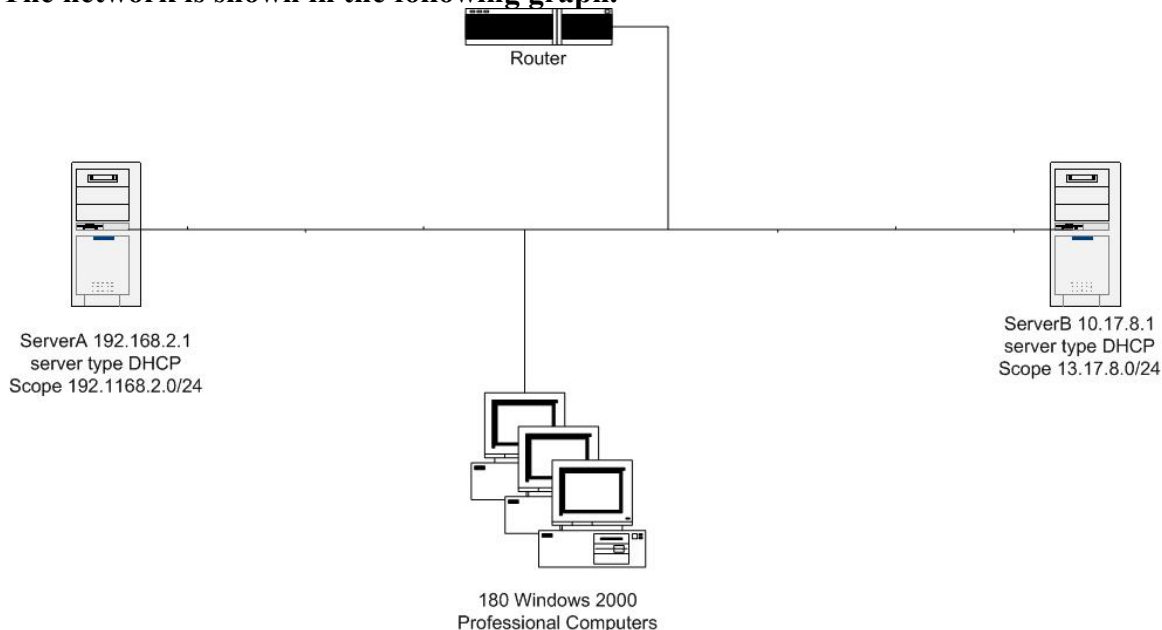
To ensure compatibility, the two address ranges will be concurrently on the same segment for three months. Routing between the two address ranges is provided by a router on the network.

After you activate the DHCP scope on the server B, users report that they are unable to obtain a valid IP address.

When you investigate the problem you discover that each of the two DHCP server responded with DHCP negative acknowledge (DHCPNACK). Messages to leases requested by the client computer.

What should you do to resolve the problem?

A. On a Windows 2000 Professional computer, disable automatic private IP addresses (APIPA)
B. On the Windows 2000 Professional computer, configure the DHCP client computers to release the DHCP lease at shutdown
C. On both DHCP server set the number of times should the DHCP server attempt conflict detection to zero.
D. On both DHCP servers configure the scope so that it has both address ranges. Define an exclusion range for the entire address range 10.17.8.0/24 on Server A and for the entire address range 192.168. 2.0/24 on server B.
E. On both DHCP servers set scope option 031. Perform router discovery to 1 to enable the option on Windows 2000 Professional computers.

Answer: D
Explanation: It is not possible to have different DHCP servers with same scopes on the same subnet. As in this scenario, they would send DHCPNACK responses to IP requests which are outside their own scope.
The solution is to replace the two scopes with a superscope which includes both scopes, and use the superscope on both DHCP servers. Precautions must be taken to prevent the scopes to overlap. This is done by exclusion ranges. We exclude the entire address range of both scopes on Server B.

Incorrect Answers:
A: Disabling APIPA would prevent clients from using APIPA addresses; instead they would get no configuration. This will not solve the problem with the two different scopes.
B: The release of IP address lease is not the problem. The problem is the two scopes on one subnet.
C: Setting the conflict detection to 0, which is the default setting, the DHCP servers would not check if an IP address is already in use, before leasing it. The two scopes are the problem, not server side conflict detection.
E: Performance router discovery is to configure routers, it is not a DHCP scope option.

QUESTION NO: 168
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. All client computers run Windows 2000 Professional.

Your network uses an IPSec policy that is defined in a Group Policy applied to all computers in the domain. You upgrade all network adapters in all computers to high-security adapters that provide encryption at the hardware level. You then delete the IPSec policy from the Group Policy.

However, you learn that the IPSec policy is still being applied to all computers in the domain. You need to ensure that the IPSec policy is removed from all computers. As your first step in achieving this goal, you create a new IPSec policy with default settings.

What should you do?

A. Assign the new policy. Run the **secedit/refreshpolicy machine_policy** command on all computers.

B.   Assign and then unassign the new policy. Run the **secedit/refreshpolicy machine_policy** command on all computers.
C.   Assign the new policy. Run the **secedit/configure /overwrite /areas securitypolicy** command on all computers.
D.   Assign and then unassign the new policy. Run the **secedit/configure /overwrite /areas securitypolicy** command on all computers.

Answer: B
Explanation: To correctly delete a policy, it should first be unassigned, and then deleted. If a policy is deleted before it is unassigned, you can assign a new policy, and then unassign it. We should then run the **secedit/refreshpolicy machine_policy** command on all computers to force a policy update.

IPSec policy will remain active even after the Group Policy object to which it is assigned has been deleted. You must unassign the IPSec policy before you delete the policy object. If you delete the policy objects and keep the policy assigned, the IPSec Policy Agent will assume it simply cannot find the policy and use a cached copy.

Reference:
IPSec Policy Is Applied After Being Deleted from a Group Policy (Q234320)
Windows 2000 Server documentation, Configure system security
Windows 2000 Server documentation, To assign IPSec policy to Group Policy

Incorrect Answers:
A: The old policy has been incorrectly deleted so we must unassign the new policy before forcing a policy update.
C: The /overwrite argument is only valid when the /CFG argument is also used.
D: The /overwrite argument is only valid when the /CFG argument is also used.

QUESTION NO: 169
You are the administrator for TestKing's Windows 2000 Server network. You company has a main office in Dallas, TX. There are three branch offices: one in Atlanta, GA, one in Chicago, IL, and one in Sacramento, CA. All branches are connected to Dallas by a T1 line. A diagram of the network in shown below:
The routers between the offices support the forwarding of BOOTP messages. At each branch office, you have a local user who is responsible for all administrative duties. Currently the local administrator is responsible for configuring the TCP/IP settings for all the Windows 2000 Professional computers at his/her local branch.

You have been experiencing network communication problems which were the direct result of configuration errors. You want to prevent this from happening again.

What should you do? (Choose two)

A.   Install and configure a Dynamic Host Configuration Protocol (DHCP) Server in Dallas.
B.   Install and configure a Windows Internet Name Service (WINS) Server in Dallas.
C.   Install and configure a Domain Name System (DNS) Server in Dallas.
D.   On each Windows 2000 Professional computer, change the TCP/IP properties to Obtain an IP address automatically.
E.   On each Windows 2000 Professional computer, change the TCP/IP properties to Obtain WINS server address automatically.
F.   On each Windows 2000 Professional computer, change the TCP/IP properties to Obtain DNS server address automatically.

Answer: A, D
Explanation: Instead of manually configuring the IP settings we should use a centralized DHCP-solution. DHCP must be installed and configured on the central Server in Dallas. Every client need to be enabled for DHCP; to obtain IP configuration automatically.

Incorrect Answers:
B: WINS is used for name resolution, not for IP configuration of clients.
C: DNS is used for name resolution, not for IP configuration of clients.
E: There is no setting "Obtain WINS server address automatically" in TCP/IP properties.
F: It would require a lot of administrative effort to configure IP configuration on each client computer. It is not the best solution.

QUESTION NO: 170
You are the network administrator for Contoso, Ltd. The network consists of three Windows 2000 domains, as shown in the exhibit.

Leading the way in IT testing and certification tools, www.testking.com
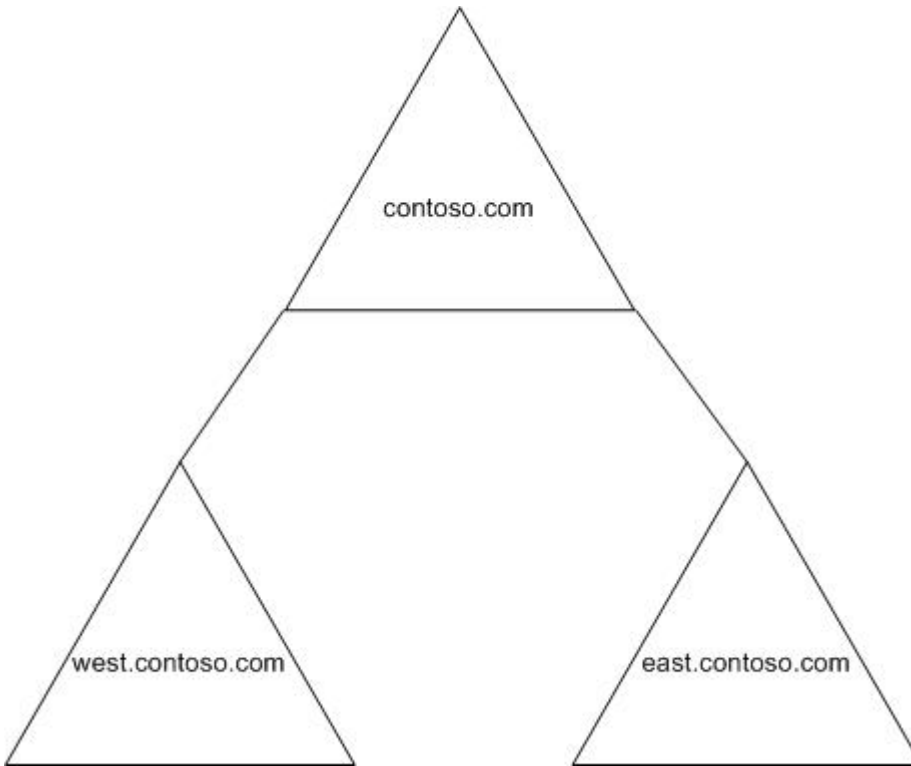
To distribute administrative control of the DNS namespace, you use a single standard primary DNS zone to handle all name resolution for the three domains. Users report that name resolution for hosts in all three domains has been extremely slow.

You want to correct this problem while still maintaining the centralized administrative control. What should you do?

  A.   Create a new primary zone for the East domain.
       Create a new primary zone for the West domain.
  B.   Create a new secondary zone for the East domain.
       Create a new secondary zone for the West domain.
  C.   Create a new Active Directory integrated zone for the East domain.
       Create a new Active Directory integrated zone for the West domain.
  D.   Create a delegated zone for the East domain.
       Create a delegated zone for the West domain.

Answer: B
Explanation: By creating secondary zones in the east and west domains, clients in the East and West domain could be configured to use the local DNS server for name resolution. This would improve performance by avoiding name resolution on the WAN links.
The administrative control would still be centralized since the secondary zone only contains read-only replicas of the primary zone file.

Incorrect Answers:
A: If primary zones were created in the East and West domain, there would be three distinct DNS zones, and it would not be possible to resolve names from different Domains.
C: Active Directory integrated zoned will not keep the DNS administration centralized. It would be possible to administer the DNS zone at the East and the West Domain.
D: Delegated zones will allow administrators in the East Domain and West Domain to administer the zones, but the zone should only be managed centrally.

QUESTION NO: 171
You are the administrator of TestKing's network. Your company consists of three offices of fewer than 30 computers each. Your company plans to expand to six offices. To accommodate the projected increase in network traffic, you decide to replace your bridges with two routers named Router 1 and Router 2. You are configuring Router 1. Which router entry should you add?

    A.   Execute route add 172.16.64.160 mask 255.255.255.224 172.16.64.129 –p
    B.   Execute route add 172.16.64.160 mask 255.255.255.240 172.16.64.129 –p
    C.   Execute route add 172.16.64.96 mask 255.255.255.224 172.16.64.97 –p
    D.   Execute route add 172.16.64.96 mask 255.255.255.240 172.16.64.130 –p
    E.   Execute route add 172.16.64.96 mask 255.255.255.224 172.16.64.130 –p

Answer: E
Explanation: Missing exhibit makes explanation impossible.

QUESTION NO: 172
You are the administrator of a Windows 2000 network. The network has two Windows 2000 Server computers named Router1 and Router2. Routing and Remote Access is enabled as a router on Router1 and Router2. There are no other routers on the network.

A part of the IP routing table of Router1 is shown in the following table.

Destination	Network Mask	Gateway	Interface	Metric
10.30.0.0	255.255.0.0	10.30.1.1	10.30.1.1	1
10.30.1.1	255.255.255.255	127.0.0.1	127.0.0.1	1
10.40.5.0	255.255.255.0	10.40.5.1	10.40.5.1	1
10.40.5.1	255.255.255.255	127.0.0.1	127.0.0.1	1

| 10.255.255.255 | 255.255.255.255 | 10.30.1.1 | 10.30.1.1 | 1 |
| 10.255.255.255 | 255.255.255.255 | 10.40.5.1 | 10.40.5.1 | 1 |

To exchange routing information, you want to enable RIP for IP on Router1 and Router2.

You configure RIP for IP on Router1 and Router2 as follows:

- Set operation mode to **Periodic update mode.**
- Set outgoing packet protocol to **RIP version 1 broadcast.**
- Set incoming packet protocol to **RIP version 1 and 2.**
- Specify Router1 and Router2 as unicast neighbors of each other.

When you monitor the IP routing table of Router2, you notice that the Server is not receiving the correct routes. What should you do?

A.   Configure RIP for IP to include host routes in announcements that are sent.
B.   Configure RIP for IP interfaces to add an input packet filter that will allow network traffic for RIP port 520.
C.   Set the RIP for IP outgoing packet protocol to **RIP version 2broadcast.**
D.   Specify Router 1 and Router 2 as RIP for IP peer routers.

Answer: C
Explanation: If a network is using a mixture of RIP v1 and RIP v2 routers, then we must configure the Windows 2000 router interfaces to advertise by using either RIP v1 broadcasts or RIP v2 broadcasts and accept either RIP v1 or RIP v2 announcements.
Router1 and Router2 are configured as unicast neighbors of each other, but only RIP Version 2 supports unicast to neighbors. By changing to only **RIP version 2broadcast,** the routers are forced to use RIP Version 2 and the routers would be able to communicate. If we are using multiple IP routing protocols, configure only a single routing protocol per interface.

Incorrect Answers:
A: There is nothing wrong with the RIP announcement. Instead the incoming router interface must be configured to only support RIP version 2.
B: Generally a filter is used to prevent traffic, and it cannot be used to allow traffic. By default, there is no protocol packet filter on the RIP for IP interface that prevents traffic on port 520.
D: By default, RIP announcements from all sources are accepted. By configuring a list of RIP peers, RIP announcements from unauthorized RIP routers are discarded. RIP peers is used for security.

QUESTION NO: 173

You are the administrator of a Windows 2000 network. The network consists of a Windows 2000 Server computer named Srv1 and 12 Windows 2000 Professional computers Srv1 has a dial-up connection that connects to the Internet.
Srv1 is configured to use Internet Connection Sharing to allow Internet access through the dial-up connection of Srv1.

The 12 Windows 2000 Professional computers are configured for static TCP/IP addressing. The IP addresses are 192.168.01 through 192.168.0.12, and the subnet mask is 255.255.255.0 The 12 Windows 2000 Professional computers have no default gateway configured.

You discover that the Windows 2000 Professional computers are not able to access the Internet through the dial-up connection of Srv1. You confirm that the preferred DNS server on the Windows 2000 Professional computers is configured correctly.
What should you do to allow all 12 computers to access the Internet through the dial-up connection of Srv1? (Choose all that apply)

    A.   On the Windows 2000 Professional computer with IP address 192.168.0.1, change the IP address to 192.168.0.13
    B.   Change the IP address on all 12 Windows 2000 Professional computers to 169.254.0.2 through 169.254.0.13
    C.   Change the subnet mask on all 12 Windows 2000 Professional computers to 255.255.0.0.
    D.   Change the default gateway on all 12 Windows 2000 Professional computers to 192.168.0.1
    E.   Change the default gateway on all 12 Windows 2000 Professional computers to 169.254.0.1

Answer: A, D
Explanation: When we enable ICS, our computer is assigned the 192.168.0.1 IP address, and if this address is already in use on another computer, ICS would thus not be able to function. This is this case in this scenario where the 12 clients got IP address in the 192.168.0.1-192.168.0.12 range. The ICS problem is solved by changing the IP address of the computer with IP address 192.168.0.1 to 192.168.0.13 and setting the default gateway to 192.168.0.1 – the IP address of the ICS computer.

Incorrect Answers:
B: ICS uses IP address in the 192.168.0.1-192.168.0.254 range, not in the 169.254.xx.xx range. APIPA uses the 169.254.xx.xx range.
C: The correct subnet mask on network using ICS is 255.255.255.0 not 255.255.0.0
E: The default gateway should be changed 192.168.0.1, which is the IP address the LAN interface of the ICS computer is assigned when ICS is enabled. The 169.254.0.1 is an IP address in the APIPA range.

QUESTION NO: 174
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The network has a persistent connection to the Internet. The relevant partition of its configuration is shown in the exhibit. (Click the Exhibit button).
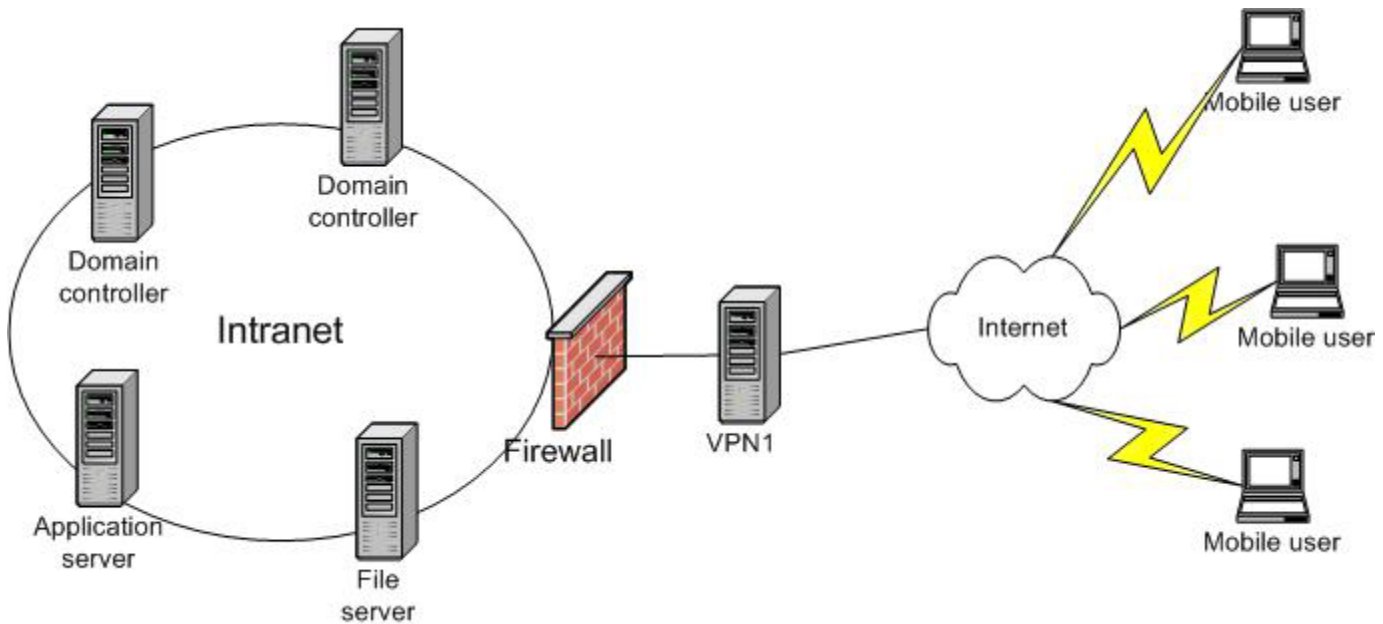
Your company employs mobile salespeople who use portable computers running Windows 2000 Professional. To enable these users to access internal resources you place a virtual private network (VPN) server named VPN1 outside your firewall. This server is a stand-alone Windows 2000 Server computer running Routing and Remote Access. The firewall is configured to allow inbound access from VPN1 only.

You configure L2TP ports on VPN1. Now you must configure additional output and input filters for the external network adapter on VPN1. You must ensure that VPN1 allows only VPN traffic on the Internet interface, and prevents non-VPN users from accessing internal resources.

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

A.   Create an input filter on VPN1 that allows L2TP ports as destination ports.
       As the destination IP address, use the IP address of the external interface of VPN1.

B.   Create an input filter on VPN1 that allows L2TP ports as source ports.
       As the source IP address, use the IP address of the external interface of VPN1.

C.   Create an input filter on VPN1 that allows L2TP ports as destination ports.
       As the destination IP address, use the IP address of the internal interface of VPN1.

D.   Create an output filter on VPN1 that allows L2TP ports as source ports.
       As the source IP address, use the IP address of the external interface of VPN1.

E.   Create an output filter on VPN1 that allows L2TP ports as destination ports.
       As the destination IP address, use the IP address of the external interface of VPN1.

F.   Create an output filter on VPN1 that allows L2TP ports as source ports.
       As the source IP address, use the IP address of the internal interface of VPN1.

Answer: A, F
Explanation:
A: The only inbound traffic allowed is traffic to the external interface on the VPN1 server.
F: The only outbound traffic allowed is traffic originating from the internal interface of VPN1.

Incorrect Answers:
B: Input filters must use the L2TP ports as destination ports, not source ports.
C: The only destination address allowed is the address of the external, not internal, VPN interface.
D: The source of an output filter must the IP address of the internal interface of VPN1.
E: In an output filter the L2TP ports must be used as a source ports.

QUESTION NO: 175
You are the administrator of TestKing's network. Your network is configured as shown in the following graph.
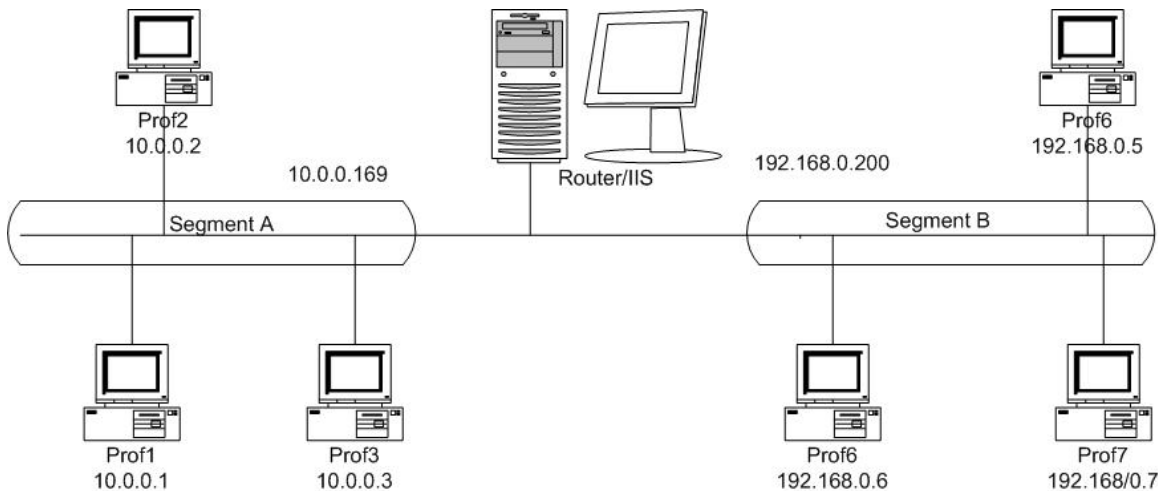
You configure your Windows 2000 Server to route all network traffic on your Intranet. Users on both segments need access to files on the other segment. A portion of the routers route table is shown in the following table.

Network destination	Netmask	Gateway	Interface	Metric
10.0.0.0	255.0.0.0	10.0.0.169	10.0.0.169	1
10.0.0.169	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.0.0	192.168.0.200	192.168.0.200	1
192.168.0.200	255.255.255.255	127.0.0.1	127.0.0.1	1

You also install and start Internet Information Services Web Service on the server. Users on both segments report they cannot access the Web service. What must you do?

A.   Disable all TCP/IP port filters

B.   Create a PPTP tunnel so that it has a filter that filters everything except protocol 6.
C.   Run the route delete 192.168.0.0 command and route add 192.168.0.0 mask 255.255.0.0 10.0.0.169 command.
D.   Run the route delete 10.0.0.0 command and route add 192.168.0.0 mask 255.0.0.0 192.168.0.200 command.

Answer: A
Explanation: A TCP/IP filter could be blocking for example TCP port 80, which is used by the HTTP protocol . By removing all filters, all traffic would be allowed to pass.

The route table is correct:
Destination 10.0.0.0 is routed to 10.0.0.169, the routers interface to the 10.0.0.0 subnet.
Destination 10.0.0.169 routes to the loopback address 127.0.0.1. 10.0.0.169 is one of the routers interfaces.
Destination 192.168.0.0 is routed to 192.168.0.200, the routers interface to the 192.16.0.0 subnet.
Destination 192.168.0.200 routes to the loopback address 127.0.0.1. 192.168.0.200 is one of the routers interfaces.

Incorrect Answers:
B: A filter that accepts PPTP but drop everything else should allow TCP Port 1723 and IP protocol 47, not protocol 6.
PPTP use TCP port 1723 for tunnel maintenance traffic. For a filter to pass PPTP data it must allow IP protocol ID 47.
C: Destination 192.168.0.0 is correctly routed to 192.168.0.200, the routers interface to the 192.168.0.0 subnet. It should not be router to the other router interface 10.0.0.169.
D: Destination 10.0.0.0 is correctly routed to 10.0.0.169, the routers interface to the 10.0.0.0 subnet. It shouldn't be deleted.
The following command gives an incorrect route: route add 192.168.0.0 mask 255.0.0.0 192.168.0.200
The network mask should be 255.255.0.0 not 255.0.0.0

QUESTION NO: 176
Your company policy is to allow only Administrators in your Houston office to install and user Network Monitor. You have been informed that Admins in New York are installing and using Network Monitor. After you install Network Monitor, what should you do to monitor how many copies of Network Monitor are currently running? (Choose two)

A.   On the Tools Menu in Net Monitor select Identify Network Monitor Users
B.   Install Network Monitor on a computer on the second segment.
C.   Remove the default Remote Access Policy
D.   Remove the "access Network Monitor" permission for Domain Admins

Answer: A, B

Explanation: We use Network Monitor to capture and display the frames that a computer running Windows 2000 Server receives from a local area network (LAN). Network Monitor can only monitor traffic on its own subnet, but by installing Network Monitor on a computer in another segment/subnet, the remote Network Monitor would be able to relay the results. By selecting the Identify Network Monitor Users command in the Tools menu in the Network Monitor program all users that is currently using the Network Monitor will be listed.

Incorrect Answers:
C: Remote Access Policy is used to control Remote Access to the computer; it is not used for monitoring the network.
D: There is no "access Network Monitor" permission" in Windows 2000.

QUESTION NO: 177
On your Windows 2000 server, you install Client Services for Netware and NWLink with the default settings. How should you configure your Windows 2000 server to connect to all Netware servers, regardless of their versions?

   A.   Set the adapter to frame type 803.2
   B.   Set the adapter to Manual Frame Type Detection and add the frame type of each Netware server.
   C.   Edit the registry to allow all frame types
   D.   You can only connect to one type of Netware server at a time so this cannot be Accomplished.

Answer: B
Explanation: On Windows 2000 computers NWLink automatically detects the frame type used by the network adapter. If multiple frame types are detected NWLink sets the frame type to 802.2. If more than one frame type must be supported the additional frame types must be added manually. This is done by the following steps on a Windows 2000 Server computer: Open Network and dial-up connections, Right click appropriate interface, select Properties, select NWLink, select Properties, select Manual frame type detection, choose Add and Select appropriate Frame Type. This setting could also be accomplished by editing the registry: add both types to the multi-string   value   PktType   in
HKLM\SYSTEM\CurrentControlSet\Services\NwlnkIPX\Parameters\Adapters\<ID>,   where   <ID>   is   the network adapter identifier

Incorrect Answers:
A: By setting the adapter frame type to 803.2 only this frame type would be allowed, not all the frame types that is used on the network.
C: There is no registry setting to allow all frame types. They must be added in the Registry one by one, which would be a daunting administrative effort.
      It is not necessary to add allow frame types, just the ones the ones used on the network.
D: This can very well be done by either adding each frame type from NWLink properties or by adding the frame types in the registry.

QUESTION NO: 178
You are the administrator of TestKing's network, which consists of two subnets, A and B. Each subnet
contains 200 client computers. Subnet A uses the network address 172.20.1.0/24. Subnet B uses the
network address 172.20.2.0/24.

You want to provide redundant DHCP service for all client computers on both subnets. You install one
Windows 2000 DHCP server on each subnet. How should you configure the scopes for each DHCP
server?

To answer, click the Select and Place button, the then drag the correct scope to the appropriate DHCP
server in ascending order. Use the minimum number of necessary scopes. You might need to use some
scopes more than once.

	Possible Scopes	
DCHP Server A		**DHCP Server B**
Scope #1	172.20.1.10 to 172.20.2.254	Scope #1
Scope #2	172.20.1.10 to 172.20.1.254	Scope #2
	172.20.1.10 to 172.20.1.200	
	172.20.1.201 to 172.20.1.254	
	172.20.2.10 to 172.20.2.254	
	172.20.2.10 to 172.20.2.200	
	172.20.2.201 to 172.20.2.254	

Answer:

Possible Scopes

DCHP Server A		DHCP Server B

172.20.1.10 to
172.20.2.254

172.20.1.10 to
172.20.1.254

DCHP Server A:
172.20.1.10 to
172.20.1.200

172.20.1.10 to
172.20.1.200

172.20.2.201 to
172.20.2.254

172.20.1.201 to
172.20.1.254

DHCP Server B:
172.20.1.201 to
172.20.1.254

172.20.2.10 to
172.20.2.254

172.20.2.10 to
172.20.2.200

172.20.2.10 to
172.20.2.200

172.20.2.201 to
172.20.2.254

Explanation: We must configure the DHCP for redundancy. We configure each DHCP server with a superscope consisting of two scopes, one scope for Subnet A (Scope #1) and one scope for Subnet B (Scope #2). We must make sure that the scopes for DHCP Server A and DHCP Server B does not overlap. We should also make sure that the IP address ranges are split according with the 80/20 (or 75/25 rule) so that the local scope uses 80% (or similar) of the local IP address rang, and the remote scope use 20% (or similar) of the remote IP address range.
Following these guidelines we conclude that:
DHCP Server A should use the scope 172.20.1.10 to 172.20.1.200 for Scope #1 (Subnet A).
DHCP Server B should use the scope 172.20.1.201 to 172.20.1.254 for Scope #1 (Subnet A).
DHCP Server B should use the scope 172.20.2.10 to 172.20.2.200 for Scope #2 (Subnet B).
DHCP Server A should use the scope 172.20.2.201 to 172.20.2.254 for Scope #1 (Subnet B).

QUESTION NO: 179
You are the network administrator for Wide World Importers. The relevant portion of your network is configured as shown in Network Configuration exhibit.
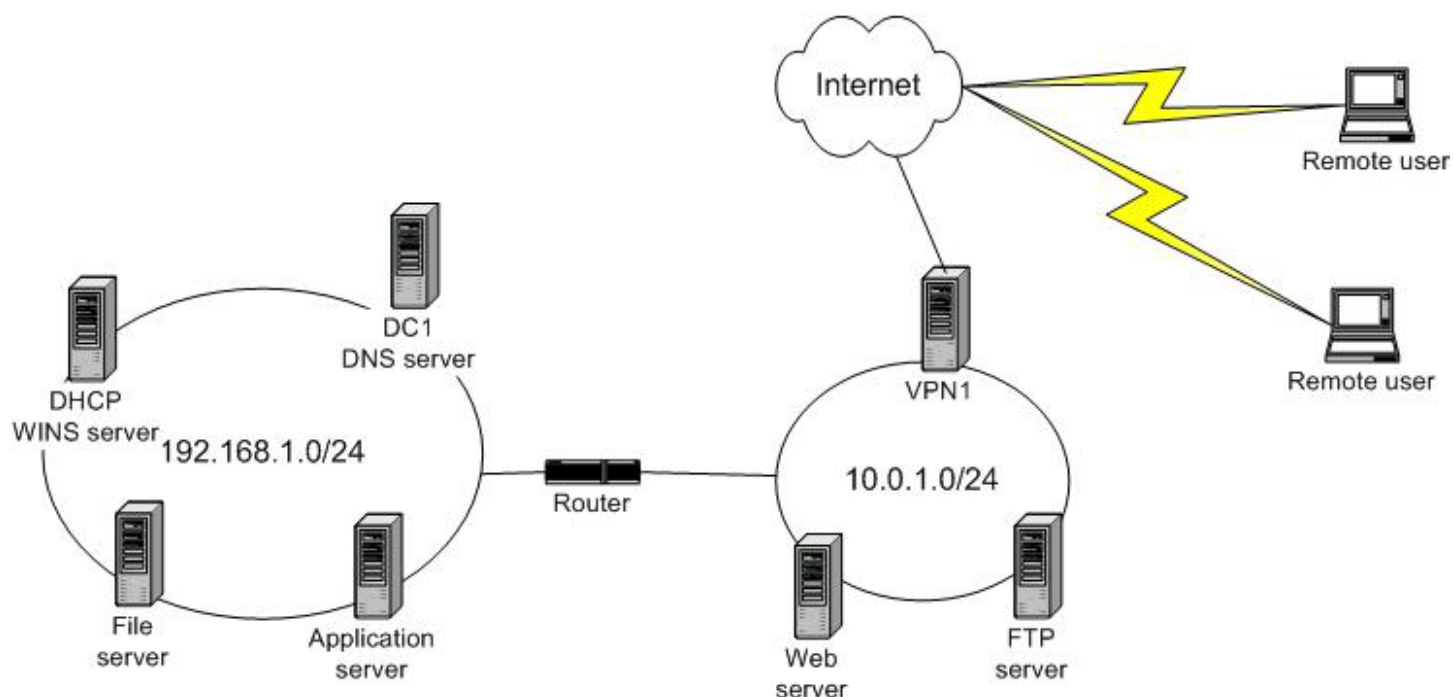
Several purchasing agents require remote access to the company network. You install Routing and Remote Access on a computer named VPN1, which runs Windows 2000 Server. You configure appropriate PPTP virtual private network (VPN) ports for remote users. You configure the IP properties of VN1 as shown in the Server properties exhibit,
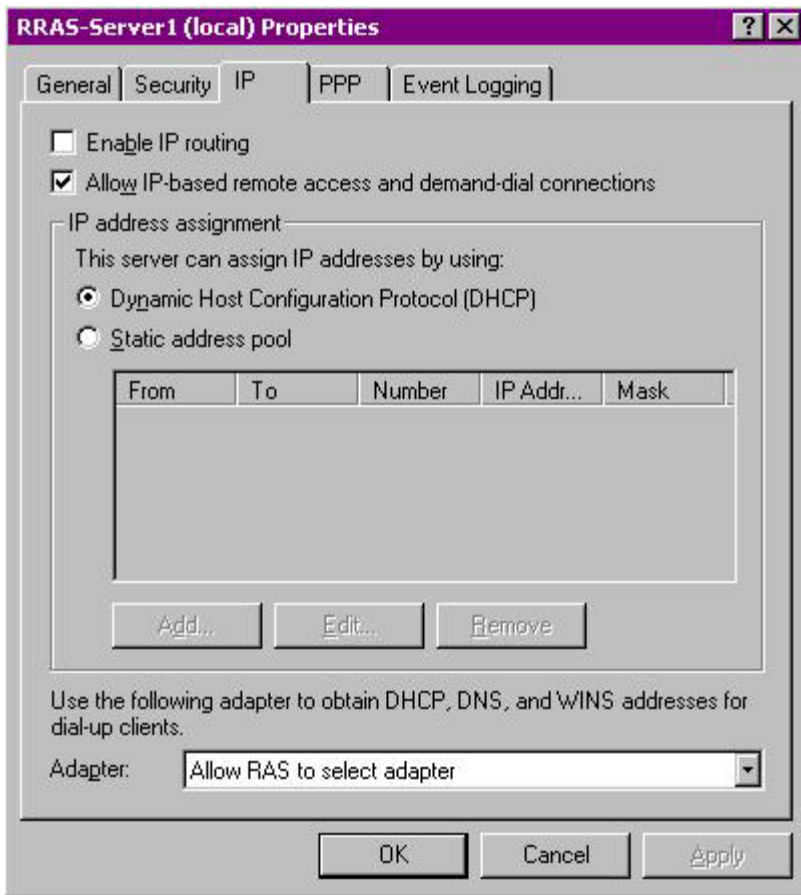
The purchasing agents now report that they can connect to VPN1, but they cannot access any network resources. On investigation, you discover that the remote computers are being configured with IP addresses in the 169.254.0.0 range.

You must ensure that the remote computers are assigned valid IP addresses on your network, and that the remote users can access network resources.

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

A. Enable IP routing on VPN1.
B. Create a static route on VPN1 to route all requests the 192.168.1.0 network.
C. Place a DHCP Relay Agent on the 10.0.1.0 network.
D. Place a DHCP Relay Agent on the 192.168.1.0 network.
E. Manually configure VPN1 with the address of the DNS server.
F. Manually configure VPN1 with the address of the WINS server.

Answer: A, C
Explanation: The clients are able to connect to VPN1, but they receive IP addresses from the APIPA, 169.254.0.0, range. They do not receive IP configuration from the DHCP server on the 192.168.1.0/24 network. We must enable DCHP traffic between VPN1 and the DHCP server.

A: To route IP traffic we must enable IP routing.

C: Some routers will not relay all DHCP traffic. These routers are known as non-BOOTP enabled (or non RFC-1541 compliant) routers. To configure DHCP between two network segments that has non-BOOTP enabled router connecting them we need a DHCP relay agent on the network segment without any DHCP server.
It seems likely that the router in this scenario is non-BOOTP enabled. We should place a DHCP Relay Agent on the 10.0.1.0 network

Incorrect Answers:
B: There is no need to configure a static route to the 192.168.1.0 network. The remote clients only need to be configured with the router as a Default Gateway.

D: The DHCP Relay Agent should not be placed on the same network segment as the DHCP server.

E: This is not a name resolution problem.

F: This is not a name resolution problem.

QUESTION NO: 180
You use a computer running Windows 2000 server and the DHCP Server service to create a DHCP scope with a lease length of 15 days and a subnet mask of 21 bits. You now want to change the configuration for the scope to have an unlimited lease and a subnet mask of 28 bits. How would you do this?

A. Delete the scope. Use the new scope wizard to create a new scope with a subnet mask of 28bits and an unlimited lease. Activate the scope.

B. Right click on the scope in DHCP and select properties. Edit the properties of the scope and change the subnet mask to 28bits and the lease to unlimited

C. Delete the scope. Use the new scope wizard to create a new scope with a subnet mask of 28 bits. Edit the properties of the new scope to set an unlimited lease. Activate the new scope.

D. Disable the scope. Edit the properties of the scope and change the subnet mask to 8 bits and an unlimited lease. Enable the scope.

Answer: C
Explanation: In this scenario the original scope must be deleted, and a new scope created. We cannot change the subnet mask of an existing scope. The New Scope Wizard does not allow us to set an unlimited lease, only maximum the value of 999. After setting the unlimited lease of the scope the scope must be activated before it can be used.

Incorrect Answers:
A: The New Scope Wizard does not let you set an unlimited lease, only maximum the value of 999.
B: We cannot change the subnet mask of an existing scope.
D: We cannot change the subnet mask of an existing scope, even if the scope is disabled.

QUESTION NO: 181
You are the network administrator for Humongouos Insurance. The relevant portion of your network configuration is shown in the exhibit.
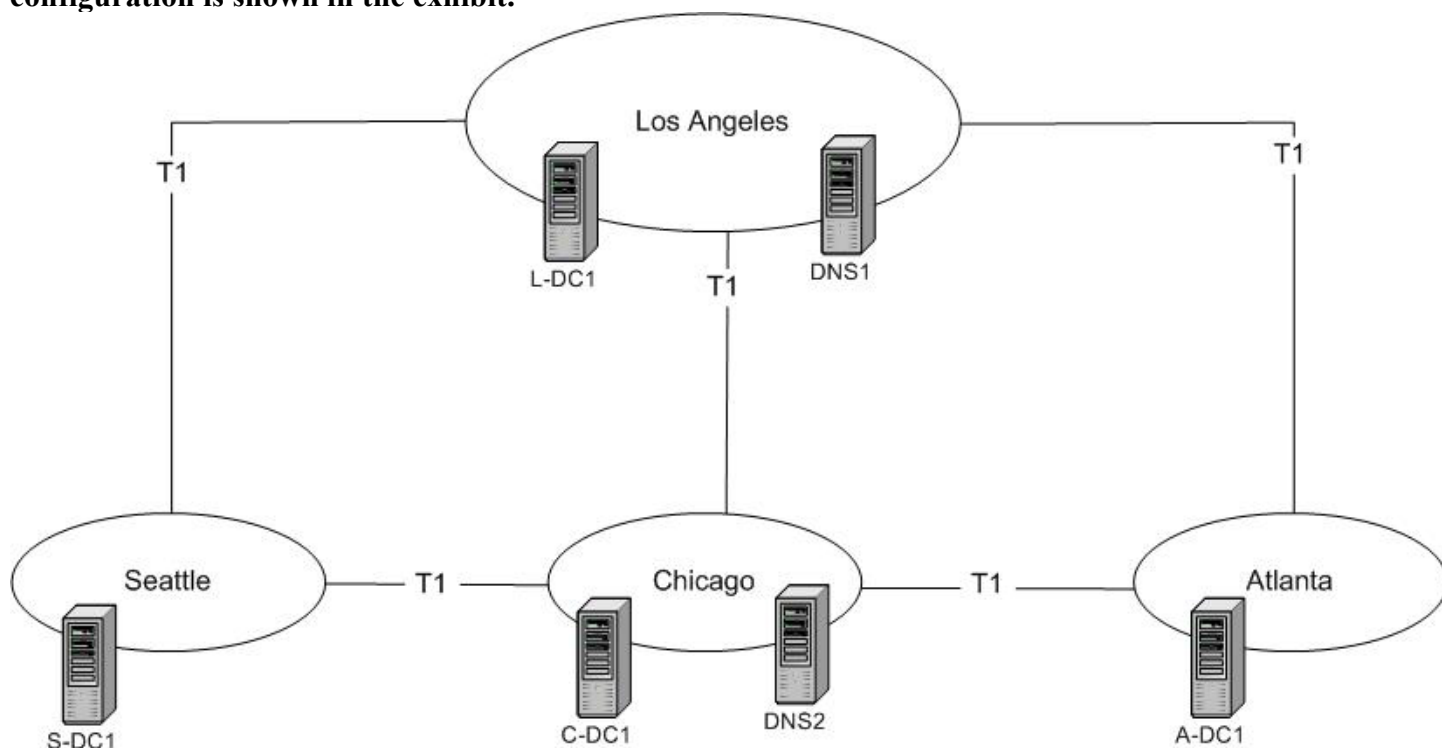
The network consists of four Windows 2000 domains, as shown in the following table.

Location	Domain name
Los Angeles	humongousinsurance.com
Seattle	west.humongousinsurance.com
Chicago	central.humongousinsurance.com
Atlanta	east.humongousinsurance.com

DNS1 hosts standard primary zones for the domains in Los Angeles and Seattle. DNS2 hosts standard primary zones for the domains in Chicago and Atlanta. Both DNS1 and DNS2 are members of their local Windows 2000 domains. Each location has its own domain controller. The domain controllers are named L-DC1, S-DC1, C-DC1 and A-DC1.

Users in Seattle and Atlanta report that access to some network resources is extremely slow in these locations, name resolution requests sometimes take longer than one minute to process. Company management expects to add more than 150 new users to each of these locations during the next few months. You are concerned that the existing DNS servers will not be adequate to handle the new users.

Leading the way in IT testing and certification tools, www.testking.com

You need to improve response times for name resolution requests in Seattle and Atlanta. You must also ensure that your DNS servers do not have a single point of failure. Your solution must take into consideration the expected growth in Seattle and Atlanta.

What should you do?

A. Install one new DNS server in Seattle and another one in Atlanta.
Configure each DNS server with a standard primary zone.

B. Install one caching-only DNS server Seattle and another one in Atlanta.
Configure both DNS servers to forward name resolution requests to DNS1 and DNS2.

C. Install the DNS Server service on the domain controllers in each domain.
Create a single Active Directory integrated zone for the entire forest on the DNS server in Los Angeles.
Remove the DNS Server service from DNS1 and DNS2.

D. Install the DNS Server service on the domain controllers in each domain.
Create an Active Directory integrated zone for each domain on its local domain controller.
Create secondary zones on each DNS server for each of the remote domains.
Remove the DNS Server service from DNS1 and DNS2.

Answer: D
Explanation: In order to improve name resolution performance we install and configure DNS server at each physical location. By creating an Active Directory integrated DNS zone for each domain at the local domain controller local name resolution would not have to cross the WAN links.
A further improvement and a solution to the single point of failure problem, is solved by creating secondary zones on each DNS server for each remote domain.
Finally we remove the DNS Server service from the old DNS servers DNS1 and DNS2.

Incorrect Answers:
A: We must remove the single point of failure. This is not achieved with this proposed solution.
B: We must remove the single point of failure. This is not achieved with this proposed solution
          Caching-only servers are used on slow WAN links, not on T1 WAN links.
C: There are several domains so we cannot create a single Active Directory integrated zone.

QUESTION NO: 182
Your network consists of 90 client computers and 50 portable computers. Computers in your network only run Windows 2000 Professional. Only 20 of the users of the portable computers will ever be in the office at the same time. You have a subnetted Class B subnet with a 25-bit mask for your network. All users need access to the Internet while in the office. How should you configure DHCP?

A.   Create 2 scopes, one for the desktop computers and one for the portables.

Leading the way in IT testing and certification tools, www.testking.com

B.   Create a superscope with 2 scopes. One scope for the desktops and one for the portables.
C.   Create a superscope with 2 user classes. Set each class with a different lease duration. Use a shorter lease for the portable computers
D.   Create one scope with 2 user classes. Set the class for the desktops with a default lease duration. Set the lease duration for the class for the portables to 1 day.

Answer: D
Explanation: The problem here is that only 7 bits (32-25) can be used for host, which only provides for 126 concurrent hosts on the network, but we have 140 computers. Therefore the IP lease duration of the LapTops should be lowered.
In this scenario we create one user class for the portable computers and one user class for the stationary office computers, each with different lease duration.

Note: User classes allow DHCP clients to differentiate themselves by specifying a User Class option. When available for client use, this option includes a user-determined class ID that can help to group clients of similar configuration needs within a scope.

Incorrect Answers:
A: You cannot configure a scope to be used by certain computers without using the user class option.
B: You cannot configure a scope to be used by certain computers without using the user class option.
C: A superscope consists of two or several scopes, not of user classes.

QUESTION NO: 183
You are the network administrator for your company. During an upgrade, you add a second network segment and a second DHCP server to the network. You name the original Segment A and the new Segment B. The network ID for Segment A is 172.16.50.0/24. The network ID for segment B is 172.16.51.0/24.

The scopes defined on each DHCP server have the characteristics shown in the following table.

DHCP server and scope name	IP address range	IP address reservations	Enable dynamic updates of DNS records?
DHCP1 172.16.50.0/24 Scope	172.16.50.10 to 172.16.50.200	MAC=00-80-C7-F8-C5-10 IP=172.16.50.10	No
DHCP1 172.16.51.0/24 Scope	172.16.51.201 to 172.16.51.254	None	No
DHCP2 172.16.50.0/24 Scope	172.16.50.201 to 172.16.50.254	None	No

DHCP2 172.16.51.0/24 Scope	172.16.51.10 to 172.16.51.200	None	No

Segment A includes an internal Web server named WEBHR. This server uses the IP address reservation for the 172.16.50.0/24 scope. Across the internal network, several Web pages contain links to WEBHR, and these links point directly to the reserved IP address.

After reboot of WEBHR, users report that all links pointing to WEBHR are broken. How should you correct this problem?

A.   Enable dynamic DNS updates on both scopes.
B.   Enable dynamic DNS updates on WEBHR.
C.   Duplicate the IP address reservation for WEBHR to the scope for segment A on DHCP2.
D.   Duplicate the IP address reservation for WEBHR to the scope for segment B on DHCP2.

Answer: C
Explanation: WEBHR has an IP address reservation on DHCP1, but not on DHCP2. When WEBHR gets a lease from DHCP1 it will get its IP address reservation, but when WEBHR gets a lease from DHCP2 it will get next free IP address, not a reserved IP address.
We must make the same IP address reservation on DHCP2, and we should make sure that the reservation is to the scope for Segment A, not Segment B, since WEBHR is located on SegmentA.

Incorrect Answers:
A: Dynamic DNS updates have nothing to do with the current problem.
B: Dynamic DNS updates have nothing to do with the current problem.
D: WEBHR is located on segment A, not Segment B.

QUESTION NO: 184
Our network consists of three network segments connected by a router. You install the DHCP server service on a Windows 2000 server. You create scopes for each subnet's range of addresses and activate the scopes. Users from the second and third subnets report they cannot connect to the network. Users on the first subnet have no problems. You check and find that the computers on segments 2 and 3 are not receiving TCP/IP information from the DHCP server. What should you do?

A.   Manually configure the IP address for the DHCP server on each client on subnets 2 and 3.
B.   Enable dynamic updates on the DHCP server
C.   Install a DHCP Relay Agent on a computer on segment 2 and 3
D.   None of the above

Answer: C
Explanation: In this scenario the clients are not able to receive IP configuration from the DHCP server. The clients use broadcasts to initiate the requests. In a subnetted network the routers must be BOOTP-enabled (or RFC 1542 compliant) to let the DHCP IP configuration traffic pass. It appears that the routers are not BOOTP-enabled, since the IP configuration works for clients on the same segment as the DHCP server, but the remote clients are properly configured. A workaround solution around the problem is to install a DHCP relay agent on each remote segment.

Incorrect Answers:
A: The clients use broadcasts to initiate the requests. They will not use the IP address of the DHCP server. There is no way to configure the IP address of the DHCP server on the client.
B: Dynamic updates are enabled on the DNS server, not on the DHCP server. No configuration of the DHCP solves the problem at hand; the users on the subnet of the DHCP have no problems.
D: The solution of this problem is to install a DHCP relay agent on each remote segment.

QUESTION NO: 185
All client computers in your domain are Windows 98 or Windows 2000. Windows 2000 users run an Internet application that accesses files on a Windows NT computer. None of your Windows 2000 computers can connect to this NT computer. But the NT computer can connect to the Windows 2000 computers. What should you do?

    A.   On the NT computer run "registerDNS" command.
    B.   On the DHCP server select Enable Updates for DNS Clients That Do Not Support Dynamic Update checkbox
    C.   On the DNS server select Enable Updates for DNS Clients That Do Not Support Dynamic Update checkbox
    D.   Run "Ipconfig /flushdns" on all of the Windows 2000 computers

Answer: B
Explanation: In this scenario, there is no mention of either DNS or DHCP in the scenario, but DNS is mentioned in every alternative and, as we shall see, the correction answer can be reached by exclusion. Windows NT clients cannot register their own A (Host) records in the DNS zone like Windows 98 and Windows 2000 clients can. This makes it impossible for clients on the network to connect to NT computers, even though Windows 98 and Windows 2000 computers can be reached all computers.
The DHCP server usually registers PTR (pointer) records when it leases IP addresses to clients. By enabling "Enable Updates for DNS Clients That Do Not Support Dynamic Update" on the DHCP serve, it will register both PTR (Pointer) and A (Host) records in the DNS zone for the Windows NT 4.0 clients. This will enable all computers to connect to the Windows NT 4.0 clients.

Incorrect Answers:

Leading the way in IT testing and certification tools, www.testking.com

A: The ipconfig/registerdns command is used to manually force a name registration or is fresh of the client name registration in DNS. This is done dynamically, but Windows NT 4.0 does not support dynamic updates so this will not work.

C: There is no "Enable Updates for DNS Clients That Do Not Support Dynamic Update" setting on the DNS server. This setting only exists on the DHCP Server.

D: Ipconfig /flushdns would clear the DNS client resolver cache. But there are no incorrect entries stored locally at the Windows 2000 clients. The problem is that the Windows NT 4.0 clients are not registered in DNS.

QUESTION NO: 186
You are the administrator of TestKing's network, which consists of a single segment and includes one DHCP server. During a network upgrade, you add a second DHCP server, a router, and a second network segment. The relevant partition of the resulting configuration is shown in the exhibit.
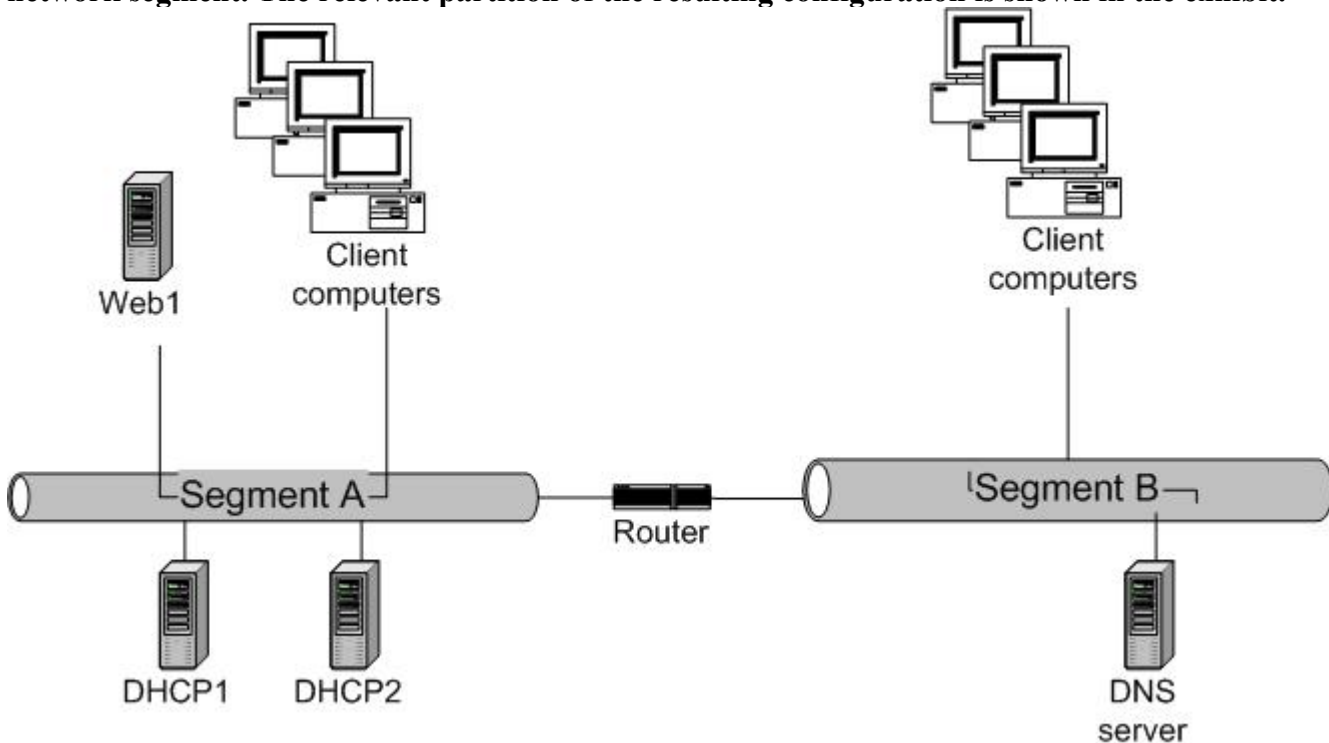
You configure the scopes on the two DHCP servers as shown in the following table.

DHCP server and scope name	IP address range	IP address reservations
DHCP1 172.16.50.0/24 scope	172.16.50.10 to 172.16.50.200	MAC=00-80-C7-F8-C5-10 IP=172.16.50.10
DHCP1 172.16.51.0/24 scope	172.16.51.201 to 172.16.51.254	None

DHCP2 172.16.52.0/24 scope	172.16.52.201 to 172.16.52.254	None
DHCP2 172.16.53.0/24 scope	172.16.53.10 to 172.16.53.200	None

Web1 runs Windows 2000 Server and Internet Information Services (IIS). This server is restarted once each week for maintenance. Web1 uses the IP address reservation on DHCP1.

You discover the following information:
- **Client computers on Segment B cannot communicate with any of the computers on Segment A.**
- **Some of the computers on Segment A cannot communicate with each other.**
- **No client computers can communicate with Web1 after it is restarted.**

You need to ensure that all client computers can communicate with each other and with Web1. What should you do?

A.   Configure an IP address reservation for Web on DHCP2. Increase the conflict detection setting on DHCP2 to **3**.
B.   Enable BOOTP forwarding on the router.
C.   Move DHCP2 to Segment B.
D.   Modify the scopes to match the scopes on DHCP1.

Answer: C
Explanation:
We have two problems in this scenario:
1. The clients on Segment B do not receive IP configuration from the DHCP servers.
2. Web1 has a reservation on DHCP1, but it does not receive this reserved IP address when it leases the address from DHCP2.
By moving DHCP2 to segment B we solve both these problems.
1. The clients on Segment B will receive IP configuration from DHCP2.
2. Web1 will one obtain leases from DHCP1. It will receive the reserved IP address.

Incorrect Answers:
A: There is no need to create an IP address reservation on DHCP2 since DHCP1 already has one reservation. Conflict detection is used in emergency situations. It would not be useful in this scenario.
B: Enabling BOOTP on the Router would only solve one problem. The clients on Segment B would be able to receive IP configuration. But Web1 could still obtain a leased address from DHCP2.
D: The scopes are correct. Two DHCP servers on the same network should not lease the same IP addresses.

QUESTION NO: 187

Your network consists of two Windows 2000 servers and 50 Windows 2000 Professional desktops. You configure DHCP server to automatically update your DNS server's forward and reverse lookup zone files with the clients' DHCP information. In the reverse lookup zone some of the client computers do not have PTR records. What should you do?

A.   Configure the DHCP server to always update DNS, even if a client computer does not request it.
B.   Enable Dynamic Updates on the DNS server
C.   Add the DHCP server to the DHCP Proxy Update list
D.   Configure the DHCP clients by putting a check mark in the "Update DNS" box on the TCP/IP properties Advanced tab.

Answer: A
Explanation: Windows 2000 clients usually register their A (Host) records in the DNS zone, and the DHCP server registers the PTR (Pointer) records. It seems like some of the clients has disabled the TCP/IP configuration setting "Register this connection's addresses in DNS", which is enabled by default. By doing this only the A (Host) record would be registered.
Since we do not know how which clients this setting has been disabled the easiest solution is configure the DHCP server to always update DNS, even if a client computer does not request it.

Incorrect Answers:
B: The A (Host) records, as it seems – no problems mentioned, are registered in the forward lookup zones, so dynamic updates must already be enabled on the DNS server.
C: There is just a single DHCP server in this scenario. The problem cannot be related to configuration of DHCP servers that are allowed to act as proxies to each other.
D: There is no "Update DNS" in the TCP/IP properties.

QUESTION NO: 188
Your network consists of a single Windows 2000 domain and uses TCP/IP. You use DHCP to assign addresses to your Windows 2000 Professional client computers. You add several new Windows 2000 Professional clients to your network. Users report that occasionally they cannot access network resources located on servers but workgroup resources are sometimes available. The TCP/IP configuration of one of the computers that is having problems shows the IP address of 169. 254. 0. 16. What should you do?

A.   Add more IP addresses to the existing DHCP scope to include enough for all client computers.
B.   Authorize DHCP in Active Directory
C.   Create a new scope to include the new clients
D.   Change the problem clients to use H mode for NetBIOS.

Answer: A
Explanation: In this scenario some client computers are unable to get IP configuration from the DHCP server, they have been assigned IP addresses in the APIPA range. The DHCP server has run out of IP addresses to lease

after the new computers have been added to the network. The best solution is to simply add more IP addresses. Scopes can be extended dynamically.

Incorrect Answers:
B: The DHCP is working since it has been able to lease addresses to other computer, but it has run out of IP addresses to lease.
C: It is not necessary to create a new scope for the new clients. Setting up a new scope could involve precise configuration and additional administrative effort.
D: DNS, not WINS, is used for IP configuration. Windows 2000 WINS clients use H-Mode by default.

QUESTION NO: 189
You install Certificate Services on two computers running Windows 2000 Server. CertRoot is an Enterprise Root Certificate Authority. CertSub is an Enterprise Subordinate CA. You have two domains: sycom.com and support.sycom.com. You add a new domain, tech.sycom.com. You attempt to issue a certificate from CertSub for a user account in tech.sycom.com. The Event Viewer shows the CA was unable to publish a certificate for tech. sycom.com\DC. DC is a domain controller for tech. sycom.com.   What   is   the   most   likely   reason   you   receive   this   error   message?

    A.   DC (tech. sycom. com domain controller) is offline
    B.   You are not a member of the Certificate Administrators for tech. sycom.com
    C.   CertSub is not a member of the group "tech.sycom.com\Cert Publishers"
    D.   The Enterprise CA is offline

Answer: C
Explanation: In this scenario a new domain tech.sycom.com is installed. There is no Certificate Authority (CA) in the tech.sycom.com domain. To be able to issue a certificate from a domain, the Server on which the CA was installed must be a member of the Certificate Publishers group of this domain. In our scenario this translates to: Certsub must be a member of Cert Publishers group in tech.sycom.com domain.

Incorrect Answers:
A: If the domain controller would have been offline another error message would be shown.
B: It is not necessary to be a member of the Certificate Administrators. The server, on which the CA was installed, must be a member of the domain from which the certificate was issued.
D: If the Enterprise CA would have been offline another error message would be shown.

QUESTION NO: 190
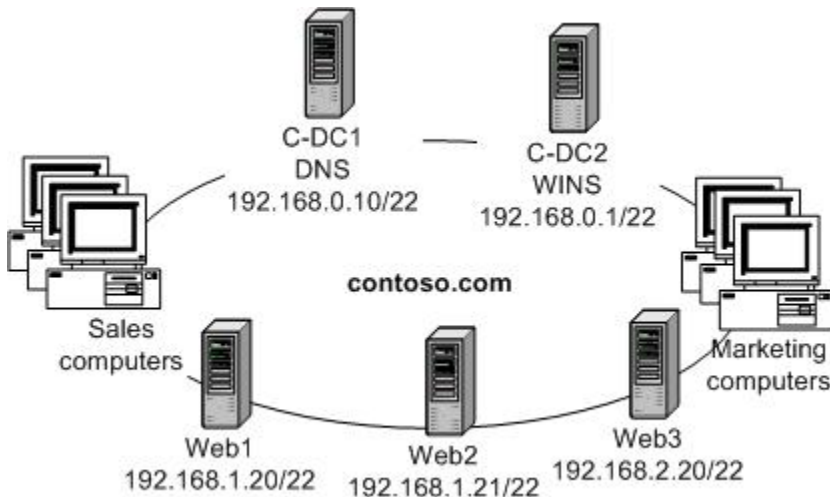
The network consists of a single Windows 200 domain and a single subnet. The network uses the addressing configuration shown in the following table.

	Network address	Subnet mask	Number of users
Infrastructure servers	192.168.0.0	255.255.252.0	n/a
Sales department	192.168.1.0	255.255.252.0	200
Marketing department	192.168.2.0	255.255.252.0	75
Managing department	192.168.3.0	255.255.252.0	25

Web1, Web2, and Web3 are Windows 2000 Server computers running Internet Information Services (IIS). These three servers host a Web application named CommodApp, which is used by the sales and marketing departments. All three servers contain identical content.

All client computers are configure to use C-DC1 for DNS name resolution and C-DC2 for NetBIOS name resolution. C-DC1 is configured with an Active Directory integrated zone. C-DC1 is also configured with three A (host) records named WebApp. These A records point to the IP addresses of Web1, Web2, and Web3.

Users in the marketing department report that access to CommodApp is extremely slow. Users in the sales and management department report no problems.

You need to improve response time to CommodApp for the marketing department. What should you do?

- A.   Install the DNS Server service on C-DC2 and create an Active Directory integrated zone.
- B.   Enable round robin DNS on C-DC1.
- C.   Disable the LocalNetPriority setting on C.DC1.

D.   Configure Web1, Web2, and Web3 as WINS clients.
E.   Configure WINS and WINS-R records on C-DC1.

Answer: C
Explanation: By default the LocalNet Priority configuration is set. It makes the DNS server prefer providing local IP addresses compared to remote IP addresses. In effect, the LocalNetPriority settings makes the DNS Server C-DC1 provide only IP address of the local Webserver Web3 (192.168.2.20) to the clients in the Sales department located on network 192.168.2.0. Web3 becomes overload. We must disable the LocalNetPriority to enable load balancing.

Incorrect Answers:
A: This would provide DNS fault tolerance, but it would not improve performance.

B: Round Robin is enabled by default. Round Robin seems to work since the users in the Sales department report no problem.

D: WINS is not a part of the problem or the solution in this scenario.

E: This is performance problem, or more specifically a load balancing problem. WINS is not a part of the problem.

QUESTION NO: 191
You are the administrator of the contoso.com network, which is configured as shown in the exhibit.
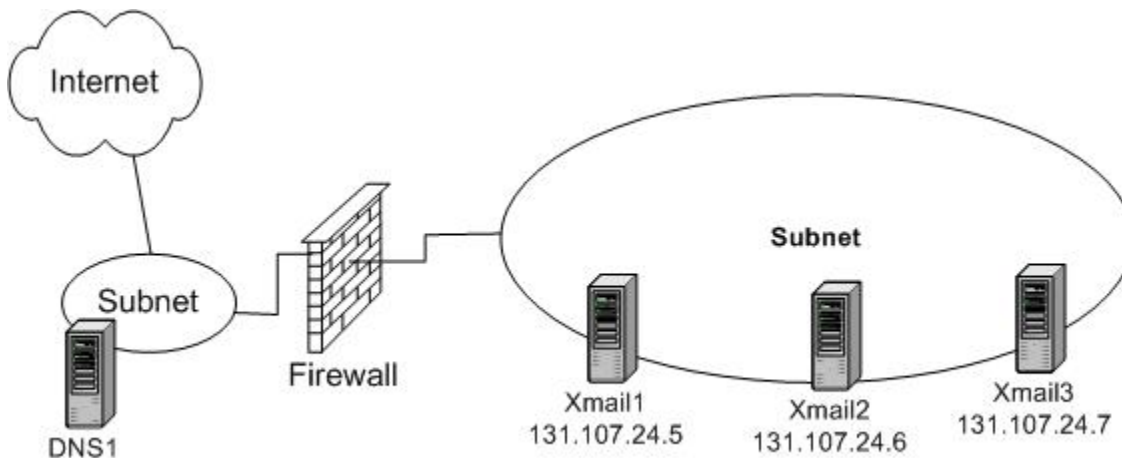
DNS1 is a Windows 2000 Server computer running the DNS Server service. Xmail1, Xmail2, and Xmail3 are Windows 2000 Server computers running Microsoft Exchange 2000 Server.

All three Exchange servers are configured to handle incoming Internet e-mail. Two servers are required to handle the volume of incoming Internet e-mail. Xmail3 contains mailboxes for company users.

Leading the way in IT testing and certification tools, www.testking.com

You want to configure DNS1 to distribute incoming Internet e-mail equally between Xmail1 and Xmail2. Of both servers become unavailable, incoming e-mail should be routed to Xmail3.

You configure DNS1 to enable round robin. How should you configure the zone file on DNS1?

To answer, drag the correct DNS configuration parameters to the appropriate locations.

Record type	Host name	IP Address
		131.107.24.5
		131.107.24.6
	Xmail3	131.107.24.7

Record types

A
MX
CNAME
SRV

Record type	Host name	Record priority
		10
		20

Host names

Xmail1	Xmail2
Xmail3	Mail

Answer:

Record type	Host name	IP Address
A	Mail	131.107.24.5
A	Mail	131.107.24.6
MX	Xmail3	131.107.24.7

Record types
A
MX
CNAME
SRV

Record type	Host name	Record priority
MX	Mail	10
MX	Xmail3	20

Host names	
Xmail1	Xmail2
Xmail3	Mail

Explanations:
We must load balance the Xmail1 and Xmail2 server. We also want redundancy. If Xmail1 and Xmail2 are unavailable we want traffic redirected to Xmail3.
We add two A (Host) records with host name Mail with IP addresses of Xmail1 and Xmail2. This would enable Round Robin Load Balancing.
We add a MX (mail) records for Xmail3. This enables internal users to use Xmail3 as e-mail server.
Finally we add two MX records, one with record priority 10 (higher priority) with Host name Mail, and one with record 20 (lower priority) with host name Xmail3. This will direct incoming Internet e-mail to Xmail1 and XMail2, or in case both Xmail1 and Xmail2 are unavailable the e-mail will be redirected to Xmail3.

QUESTION NO: 192
You have three Windows 2000 domain controllers in a single domain. Your primary DNS server is installed on a domain controller named dc1.sycom.com. You have two secondary DNS servers installed on member servers named srv1.sycom.com and srv2.sycom.com. You want to increase fault tolerance for your DNS infrastructure. You also want to optimize and simplify replication and zone transfer management on your network. What should you do? (Choose all that apply)

   A.   Remove the DNS service from the member servers
   B.   Install DNS on at least 2 more domain controllers.
   C.   Convert the zone to an Active Directory integrated zone.
   D.   Promote one of the secondary DNS servers to a primary server and have it host a new zone.
   E.   Configure secure updates for your zone transfers

Answer: A, B, C

Explanation: By installing DNS on 2 more domain controllers, coping the DNS zone from the member servers to the domain controllers, removing the DNS service from the member servers, and converting the zone to an Active Directory zone we have accomplished a migration from a primary DNS zone to an Active Directory zone. The benefits of this are increased fault tolerance as both DNS server would have a replica of the DNS zone; simplified replication as the zone replication is integrated in the Active Directory replication and does not have to be configured or managed; optimized replication as Active Directory replication is performed on a per-property basis and only relevant changes are propagated therefore less data to be used and submitted in updates for directory-stored zones; and secure zone transfers as Active Directory replication uses secure channels, which provide encryption.

Incorrect Answers:
D: If we use two primary DNS servers for two separate zones, they would not be able to communicate, and there would be no cross-domain name resolution and therefore no fault tolerance.
E: Zone transfers cannot be configured for secure updates. Only updates of zone records, not zone transfers, can be configured for secure updates. We cannot have secure zone transfers if we are not using Active Directory integrated zones.

QUESTION NO: 193
You configure DHCP to dynamically update the PTR records for clients who lease IP addresses from the server. From where is the domain name used in the PTR record obtained?

    A.   From the DHCPDISCOVER message
    B.   From the DHCPOFFER message
    C.   From the DHCPACK message
    D.   From the DHCPREQUEST message

Answer: D
Explanation: In the DHCP Lease process the client that requires an IP address broadcasts a DHCPDISCOVER. DHCP server responds by sending DHCPOFFER to which the client answers with a DHCPREQUEST. The client's Fully Qualified Domain Name (FQDN) is included in the DHCPREQUEST message. This could be used by DHCP server to update the PTR (Pointer) record of the client. The DHCP server then acknowledges the lease with DHCPACK.

Incorrect Answers:
A: The DHCPDISCOVER message is a broadcast from the client. It does not include the clients FQDN.
B: The DHCPOFFER message is send by the DHCP server. The FQDN is supplied by the client.
C: The DHCPACK message is send by the DHCP server. The FQDN is supplied by the client.

QUESTION NO: 194

Your network consists of computers running Windows 2000 server, Windows 2000 Professional, Windows 95 and OS\2 with LAN Manager 2. 2c. All are on the same subnet. You want applications on the OS/2 client that use NetBIOS names to be able to resolve the NetBIOS names to IP Addresses from a WINS database. You install WINS on one of the Windows 2000 servers. What else should you do to enable the applications on the OS/2 computer to resolve NetBIOS names to IP addresses from the WINS database?

A.   Configure one of the Windows 2000 Professional computers as a WINS Proxy Agent.
B.   Add static mappings for the OS/2 computer in the WINS database.
C.   Configure the OS/2 computer as a WINS Client.
D.   Configure the OS/2 computer with a static IP address and add a PTR record in the
       DNS database

Answer: A
Explanation: In this scenario LAN Manager 2.2c with OS/2 is not able to act as a WINS client to a WINS server on a remote subnet. This is because OS/2 clients only broadcast for WINS. To reach a WINS server on remote subnets a WINS Proxy agent, which can be installed on a Windows 2000 Professional computer, will capture those broadcasts and relay them to the WINS Server.

Incorrect Answers:
B: By adding a static mapping of the OS/2 computer, the clients would be able to connect to the OS/2 computer. This is not the requirement in this scenario though.
C: The OS/2 computer is already configured as a WINS client but it can only use broadcasts to connect to a WINS server, which makes it impossible for it to reach a WINS server on a remote subnet.
D: Giving the OS/2 computer a static IP address, and adding a PTR (pointer) record of it in DNS, would not enable it connect to the WINS server.

QUESTION NO: 195
Your Windows 2000 network has 3 subnets, A, B, and C. A is at the corporate headquarters.

B is used to connect a router at the HQ office to a router at the remote office. C is the subnet for the remote office. You use two Windows 2000 servers as routers: RouterAB connects SubnetA and SubnetB. RouterBC connects subnetB and subnetC. You configure RouterAB and RouterBC to use demand-dial connections.

What two steps must you take to allow a client computer on SubnetC to access a share on a client on SubnetA? (Choose Two)

A.   Configure TCP/IP filter on the RouterAB demand-dial interface
B.   Configure a static route for SubnetA on the demand-dial interface of RouterBC
C.   Configure a static route for SubnetB on the demand-dial interface of RouterAB

D.   Configure TCP/IP filter on the RouterBC demand-dial interface

Answer: B, C
Explanation: In this scenario there is a small network with only 3 subnets. The most practical solution for a small network would be to configure the routers with static routes. However, static routes do not scale well for larger internetworks.
In this scenario subnet B is already connected to both of the routers so no further routes to subnet B has to be made. Subnet A is connected to the RouterAB but not to the router BC. We have to configure a static route on Router BC to subnet A. Subnet C is connected to the RouterBC but not to the router AB. We have to configure a static route on Router AB to subnet C.

Incorrect Answers:
A: In this scenario we have a Routing problem, not a traffic filter problem. Static routes, not TPC/IP should be used.
D: In this scenario we have a Routing problem, not a traffic filter problem. Static routes, not TPC/IP should be used.

QUESTION NO: 196
Your domain has a Windows 2000 member server computer named Srv1. Routing and Remote Access and CHAP are enabled for remote access on Srv1. You have also configured the appropriate remote access policy to use CHAP. However, users who require CHAP report that they are not able to dial into SRV1. What should you do?

A.   Configure SRV1 to disable LCP extensions
B.   Configure clients to use MSCHAP for dial in
C.   Configure SRV1 to use SPAP for dial in
D.   Disable "Mutual authentication" on SRV1

Answer: A
Explanation: If we cannot connect to a server by using PPP, or the remote computer terminates our connection, the server may not support LCP extensions. In Network and Dial-up Connections, clear the Enable LCP extensions check box.

Incorrect Answers:
B: Both the Remote Access Policy and the client is configured to use CHAP. Configuring the client to use MS-CHAP would not make any difference.
C: The client is configured to use CHAP. Configuring SRV1 to use SPAP for dial-in would not allow communication. Both client and server must use the same authentication protocol.
D: CHAP does not support mutual authentication, so disabling mutual authentication will not help.

QUESTION NO: 197
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain that
spans three network segments. The relevant portion of its configuration is shown in the exhibit.
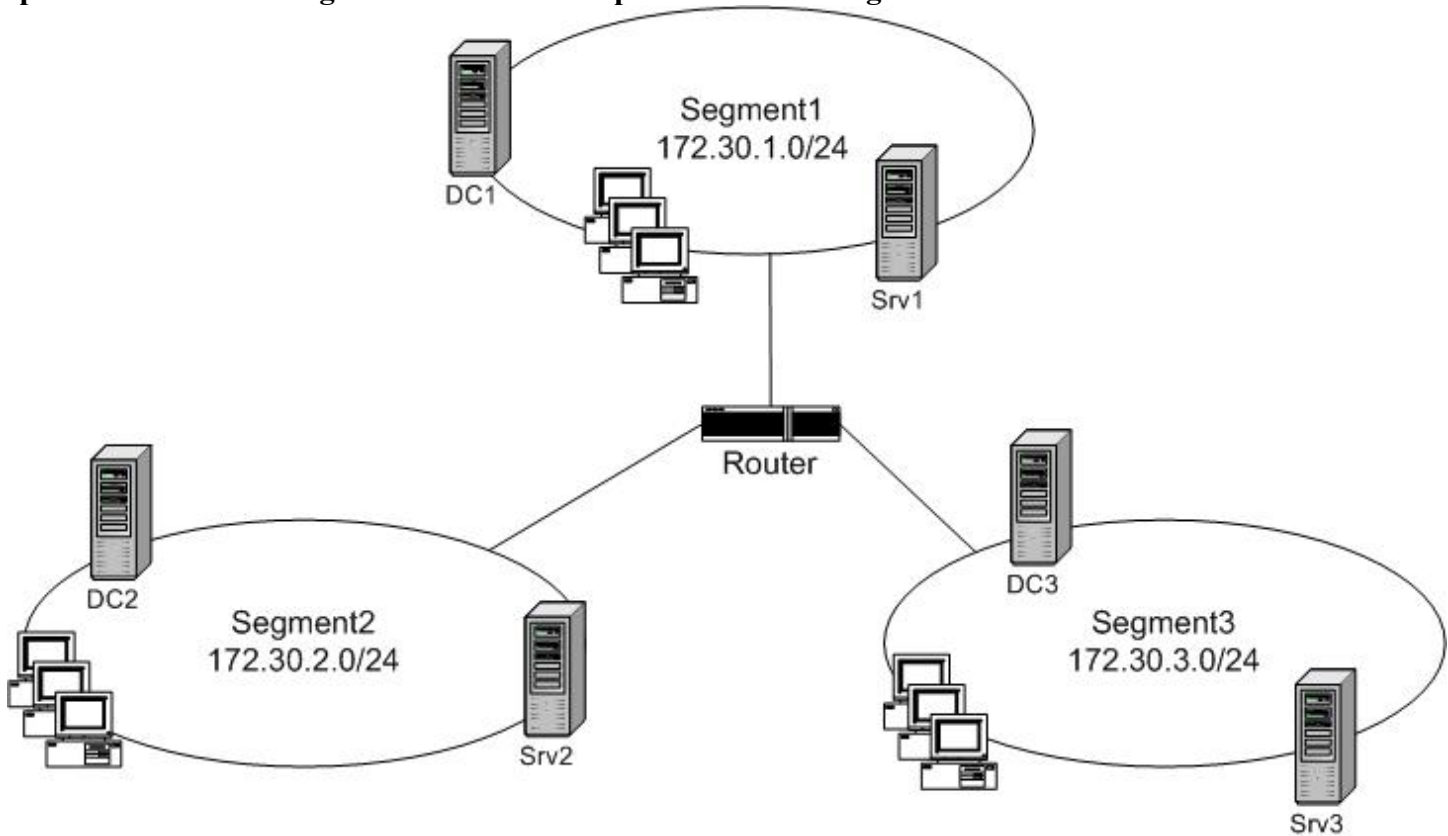
The router is configured in the following table.

Interface	Segment	IP address
Interface 1	Segment1	172.30.1.1/24
Interface 2	Segment2	172.30.2.1/24
Interface 3	Segment3	172.30.3.1/24

Each segment contains one Windows 2000 domain controller and one Windows 2000 member server. The
domain controllers are named DC1, DC2, and DC3. Each domain controller runs the DNS Server service
and hosts an Active Directory integrated zone. DC1 also runs WINS.

Each segment contains 100 client computers running Windows 2000 Professional. All client computers
have static IP addresses.

A user named Paul, on Segment2, reports access problems. When he tries to access shares on Srv1 and
Srv3, he receives the following error message: "Network path not found". He can successfully connect to
resources on Segment2. No other users report problems.

You run the ipconfig /all command on Paul's computer and receive the following information.

Windows 2000 IP configuration:	
Host Name	Laptop-1
Primary DNS Suffix	Graphicdesigninstitute.com
Node Type	Hybrid
IP Routing Enabled	No
WINS Proxy Enabled	No
DNS Suffix Search list	Graphicdesigninstitute.com
Ethernet adapter Local Area connection:	
Connection-specific DNS Suffix	
Description	Xirxom Ethernet Adapter 10/100
Physical Address	00-80-C7-E4-2B-DC
DHCP Enabled	No
IP Address	172.30.2.201
Subnet Mask	255.255.0.0
Default Gateway	172.30.2.1
DNS Servers	172.30.2.10
Primary WINS Server	

To correct the connectivity problem, you decide to configure Paul's computer. What should you do?

- A. Enable IP routing.
- B. Change the subnet mask to 255.255.255.0
- C. Add the address of the DNS servers in Segment1 and Segment3 to the advanced IP properties.
- D. Add the address of the WINS server on Segment1 to the advanced IP properties.
- E. Add additional default gateways of 172.30.1.1 and 172.30.3.1.

Answer: B
Explanation: Paul has an incorrect subnet mask. The segments use a 24-bit network mask (both the exhibit and the routing table indicates this fact), not a 16-bit network which is configured on Paul's computer.

Incorrect Answers:
A: The client computer should not be used as a router.

C: Paul can use the DNS server on Segment2 (he can access resources on Segment2). Since all DNS server host the same Active Directory Integrated zone, they all contain the same zone and the same records. It was not be useful to add the addresses of the other DNS servers.

D: All computers are Windows 2000 and the DNS servers are running in Active Directory integrated mode. WINS is unlikely the cause here. He is able to access resources in segment 2.

E: There can only be one single Default Gateway, not three.

QUESTION NO: 198
You are the administrator of TestKing's network, which consists of a single Active Directory domain in native mode. All servers on the network run Windows 2000 Server. Client computers run either Windows 2000 Professional, Windows 98, or Windows 95. All client computers use DHCP for IP addressing and configuration. All servers have static IP addresses. The DHCP servers are configured to perform registration of DNS records for client computers.

You change your DNS zones to Active Directory integrated zones and upgrade all client computers to Windows 2000 Professional. Users report that they can no longer access some network resources. IP addresses are leased by the DHCP servers, but not all A (host) records for the leased addresses of the upgraded client computers exist in the DNS zone.

You must enable users to access all the network resources they need. What should you do?

A. Disable the option for DHCP servers to register DHCP clients with the DNS servers.
B. Reauthorize all DHCP servers in Active Directory.
C. Add the DHCP servers to the DnsUpdateProxy group in Active Directory.
D. Require secure dynamic updates for the existing zones.

Answer: C
Explanation: Ordinarily only the owner of the DNS record would be able to delete or update it. Now we must allow all DNS servers to change and delete these client DNS records. The solution to this problem is to use Active Directory Users and Computers to add your DHCP server computers to the built-in DnsUpdateProxyGroup. This will permit all of your DHCP servers the right to perform proxy updates for any of your DHCP clients.

Incorrect Answers:
A: The DHCP servers only register downlevel clients like Windows 2000 and Windows 95. After the upgrade all client computers are Windows 2000. Disabling the option to register DHCP clients with DNS would have no effect.
B: The DHCP servers have already been authorized in the Active Directory. They were working before the upgrade of the DNS zones.
D: To require secure updates would not help.

QUESTION NO: 199
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. Your network includes 200 desktop client computers. Some of these computers run Windows 2000 Professional, and the rest run Windows NT Workstation 4.0. All client computers use DHCP to obtain

their TCP/IP configuration. DHCP is configured to dynamically register DNS records for all DHCP clients.

Five mobile users require remote access to network resources. Two of the five users have portable computers that run Windows 2000 Professional. The other three users have portable computers that run Windows NT Workstation 4.0.

You install Routing and Remote Access on a server, accepting all default settings. You configure two network adapters named NIC1 and NIC2 on this server. NIC1 is connected to the Internet and NIC2 is connected to the internal network. You ensure that your DHCP server has enough IP addresses to accommodate all DHCP clients.

The two remote users who use Windows 2000 Professional can now successfully connect to the remote access server. However, the other three remote users report that they are sometimes unsuccessful when they try to connect to the remote access server.

How should you correct this problem?

   A.   Configure the remote access server to use NIC1 to obtain DHCP configuration.
   B.   Configure the remote access server to use NIC2 to obtain DHCP configuration.
   C.   Create a new DHCP scope for the remote users and set the DHCP lease duration to be unlimited.
   D.   Create a new DHCP scope for the remote users and set the DHCP lease duration to be one hour.

Answer: B
Explanation: The remote access server should be configured to use the internal interface, NIC2, to obtain IP configuration.

Incorrect Answers:
A: NIC1 is the external interface on the RAS server. DHCP configuration is provided by the DHCP server which is located on the internal network. NIC2, not NIC1, connects to the internal network on the RAS server.
C: It would be unwise to have an unlimited lease duration. In effect the clients would use static IP addresses. Furthermore, the lease duration has nothing to do with the problem at hand.
D: Decreasing the lease duration would not enable the NT clients to connect.

QUESTION NO: 200
You are the administrator of a Web server hosted on the Internet that runs on a Windows 2000 Server. You want to download ActiveX controls automatically to your customers' Internet browsers. The default security settings on your customers' browsers prevent this. What should you do to automate the downloading of your ActiveX controls?

A.   Install an Enterprise CA on one of your domain controllers and have it issue a certificate for code signing.
B.   Install an Enterprise Subordinate CA that uses a commercial CA as the parent. Create a policy on the Subordinate CA that allows the Web developers to request a certificate for code signing.
C.   Install an Enterprise CA on one of your domain controllers. Install an Enterprise Subordinate CA on one of your member servers. Issue code-signing certificates to your Web developers.
D.   Configure your Web server to request code signing certificates from a commercial CA such as Verisign.

Answer: D
Explanation: Only external customers will use the certificates. It is not necessary to have a Certification Authority (CA) connected to the domain. The best solution is to use certificates from a commercial CA such as Verisign.

Incorrect Answers:
A: External customers would not be able to use an Enterprise CA since they are not a part of your domain.
B: The certificate must be issued by the public CA, not the subordinate Enterprise CA, to be able to be used by external customers with no rights or permission in the domain.
C: External customers would not be able to use an Enterprise Subordinate CA that uses an Enterprise CA, since they are not part of the domain.

QUESTION NO: 201
You are the network administrator for the Research department of TestKing Pharmaceuticals. The Windows 2000 domain structure of your network is shown in the exhibit.
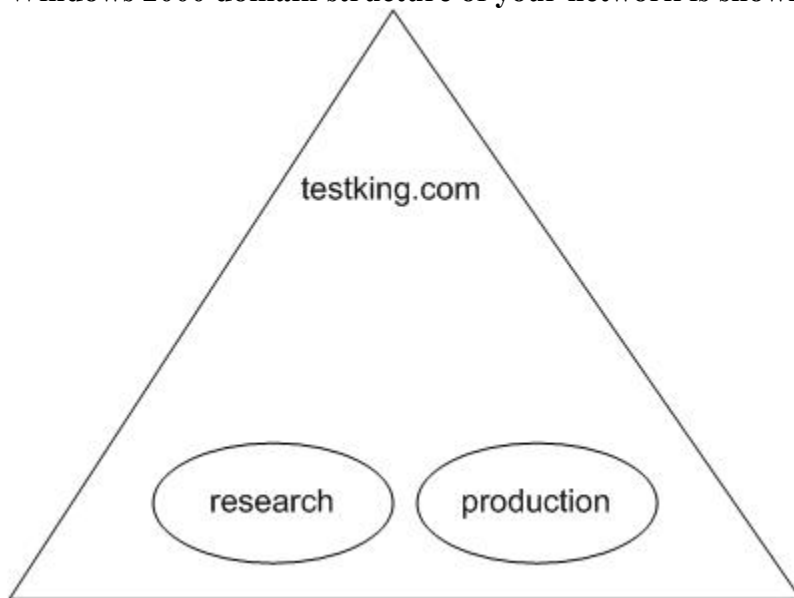
You need to set up a DHCP server for a new Windows 2000 lab in your department. You install a Windows 2000 Server computer as the first domain controller in a domain named research.testking.com. You then install and configure DHCP services on the new server.

You ask Lilleanne, a member of the Enterprise Admins group for testking.com, to authorize the new DHCP server. She tries to do so. However, she receives an error message stating that the server cannot be located in the directory for testking.com.

You need to ensure that your DHCP server is properly authorized in the directory for contoso.com. What should you do?

    A.   Create a one-way trust relationship from contoso.com to research.com.
    B.   Add the Enterprise Admins group for contoso.com to the Administrators group for research.contoso.com.
    C.   Run dcpromo.exe on the DHCP server and join it to the contoso.com domain.
    D.   Create a one-way trust relationship from research.contoso.com to contoso.com.

Answer: B
Explanation: Only members of the Administrators group in the local domain can authorize DHCP servers in the Active Directory.

Incorrect Answers:
A: There already, by default, exists a two-way trust between the domains since both domains are in the same domain tree. Furthermore this explicit trust would be in the incorrect direction.
C: Active Directory is already installed on the DHCP server which is a domain controller in the research.contoso.com domain.
    You can't simply move a domain controller from one domain to another by running dcpromo.exe.
    Note: To migrate from one domain to another the dcpromo.exe utility would have to be used twice. First to remove AD while leaving the 1st domain, and then adding AD while joining the 2nd domain.
D: There is no need to add an explicit trust. There already, by default, exists a two-way trust between the domains since both domains are in the same domain tree.

QUESTION NO: 202
You are the administrator for your TestKing's network. Your network has three Windows 2000 Server computers, named Srvr1, Srvr2, and Srvr3. Each employee has his own Windows 2000 Professional computer. Also there is one Windows 2000 Professional computer, named Prof1 that is used by the general public. Recently several files have been written to Srvr1 and Srvr2 that could have possibly caused great harm to TestKing's network. You suspect that the files came from Prof1. You want to monitor the traffic between these three computers. Srvr3 is located in your office so you decide to capture the data there. You want to accomplish these goals with the least amount of administrative overhead. What should you do?

Leading the way in IT testing and certification tools, www.testking.com

A.   On Srvr3, install the Network Monitor Tools. Then start Network Monitor and configure the capture data for Prof1, Srvr1, and Srvr2.
B.   On Prof1, install the Network Monitor driver. On Srvr1 and Srvr2, install the Network Monitor driver. On Srvr3, install the Network Monitor Tools. Then start Network Monitor and configure the capture data for Prof1, Srvr1, and Srvr2.
C.   On Prof1, install the Network Monitor Tools. Then start Network Monitor and configure capture data for Prof1. On Srvr1 and Srvr2, install the Network Monitor driver. On Srvr3, install the Network Monitor Tools. Then start Network Monitor and configure the capture data for Srvr1 and Srvr2.
D.   On Prof1, install the Network Monitor driver On Srvr1 and Srvr2, install the Network Monitor Tools. Then start Network Monitor and configure the capture data for Srvr1 and Srvr2, respectively. On Srvr3, install Network Monitor Tools. Then start Network Monitor and configure the capture data for Prof1.

Answer: B
Explanation: In this scenario we should install the Network Monitor tools on the computer we want to use to capture data to, i.e. Srv3, and install the network monitor driver on the computers we want to monitor, i.e. Srvr1, Srv2 and Prof1.

Incorrect Answers:
A: The Network Monitor driver must be installed on all computers from where you want to capture data.
C: You cannot install the Network Monitor Tools on a Windows 2000 Professional computer; a Windows 2000 Server computer is required.
D: The traffic you need to capture is between Srv1, Srv2 and Prof1. By only capturing data from Prof1 you will not capture any communication between Srv1 and Srv2.

QUESTION NO: 203
You are the administrator of TestKing's network. You have a portable computer that uses Microsoft Internet Explorer to access TestKing's Internet Information Services (IIS) computer. This application works successfully when your portable computer is docked at the office, but it fails when your portable computer is connected by Routing and Remote Access. You want to configure your portable computer to connect to TestKing's network by Routing and Remote Access. You want to install only what is necessary while maximizing performance and minimizing administrative overhead. Which box or boxes should you click in the Networking tab of the dialog box? (Choose all that apply)

A.   Internet Protocol (TCP/IP)
B.   File and Printer Sharing for Microsoft Networks
C.   Network Load Balancing
D.   Client for Microsoft Networks

Leading the way in IT testing and certification tools, www.testking.com

Answer: A, D
Explanation: The TCP/IP protocol is needed to remotely access the IIS computer. The IIS application works when the computer is docked at the LAN, but it does not function when you are connecting remotely through the RRAS server. The IIS server requires Kerberos Authentication, which is through a user account in the domain, and therefore the Client for Microsoft Networks must be configured on the remote connection on the laptop.

Incorrect Answers:
B: There is no requirement that the user of the laptop should be able to share files and printers on the laptop.
C: We cannot configure Network Load Balancing on a remote connection.
Network Load Balancing (NLB).
NLB balances the workload among each server by allowing the group of servers to be addressed by the same set of Internet Protocol (IP) addresses.

QUESTION NO: 204
You are the administrator of a Windows 2000 domain. The domain has two Windows 2000 member server computers named Istanbul and Rome. Routing and Remote Access is enabled for remote access on Rome. Internet Authentication Service (IAS) is installed on Istanbul. Rome uses Istanbul to authenticate remote access credentials. The remote access policies on Istanbul specify that domain members are allowed remote access to the network. However, users report that they are not allowed to dial in to Rome. When you investigate the problem, you discover that the configuration of Istanbul supports only local user accounts.
What should you do?

   A.   Add Istanbul to the RAS and IAS Servers group in Active Directory
   B.   Configure Routing and Remote Access on Istanbul to use RADIUS Authentication
   C.   On Istanbul, add a realm replacement rule for the Windows 2000 domain
   D.   On Istanbul, add a remote access policy that uses MS-CHAP

Answer: A
Explanation: If the remote access server is a member server in a Mixed-mode or Native-mode Windows 2000 domain and is configured for Windows authentication, the computer account of the RAS server computer must be a member of the RAS and IAS Servers security group.
Configuring membership can be performed by a domain administrator by using the Active Directory Users and Computers snap-in to add the computer to the RAS And IAS Servers security group in the Users container.

Incorrect Answers:
B: This is not an authentication problem. The problem is that the configuration of IAS on Istanbul only supports local user accounts.

C: Realm replacement rules are used to transform user credentials, for example by replacing the user name someone@business with someone@business.au. Then IAS will forward the authentication request as someone@business.au. But the problem is that the configuration of IAS on Istanbul only supports local user accounts.

D: This is not a Remote Access Policy problem. The problem is that the configuration of IAS on Istanbul only supports local user accounts.

QUESTION NO: 205
You are the administrator of a Windows 2000 network that consists of a single domain. Because no employee in your company should have the ability to encrypt files by using Encrypting File System (EFS), you need to remove this ability from all users in the domain. What should you do to accomplish this goal? (Choose all that apply)

A. From the Run command, start Secpol.msc
B. Go to the Encrypted Data Recovery Agents container and delete the certificate you find. From the Active Directory Users and Computers console, access the Group Policy Editor and edit the domain policy.
C. Go to the Public Key Policies container and delete the Encrypted Data Recovery Agents policy. From the Active Directory Users and Computers console, access the Group Policy Editor and edit the domain policy.
D. Go to the Encrypted Data Recovery Agents container and delete the certificate you find
E. Go to the Encrypted Data Recovery Agents container and initialize the empty policy. From the Active Directory Users and Computers console, access the Group Policy Editor and edit the domain policy
F. Go to the Public Key Policies container and initialize the empty policy

Answer: D, E
Explanation: The ability to encrypt files must be removed from all users in the domain. This is done by going to the Encrypted Data Recovery Agents container and deleting the certificate we find there, going to the Encrypted Data Recovery Agents container and initializing the empty policy; and from the Active Directory Users and Computers console, accessing the Group Policy Editor and editing the domain policy. There is a difference between an empty policy and no policy. In Active Directory where the effective policy is an accumulation of Group Policy Objects defined at various levels in the directory tree, the absence of a recovery policy at higher-level nodes (for example, at the domain node) allows policies at a lower level to take effect. An empty recovery policy at higher-level nodes disables EFS by providing no effective recovery certificates. On a given computer (stand-alone or joined to the domain), an effective policy must have at least one valid recovery certificate to enable EFS on that computer. Furthermore, the EFS Policy has to be deleted.

Incorrect Answers:
A: There is no command tool or Microsoft Management Snap-in called Secpolmsc.
B: An empty policy must be initialized. If not, other policies could take effect and enable EFS.

Leading the way in IT testing and certification tools, www.testking.com

C: The Encrypted Data Recovery Agents policy is contained in the Encrypted Data Recovery Agents container, not in Public Key Policies container.
The empty policy must be initialized.
F: The empty policy is initialized in the Encrypted Data Recovery Agents container, not the Public Key Policies container. The EFS Policy has to be deleted

QUESTION NO: 206
You are the administrator of a Windows 2000 domain. The domain has a Windows 2000 member server computer named TestKingA. Routing and Remote Access is enabled for remote access on DeskA. Your company is organizing an industry trade show in a conference center. You have set up 15 desks and telephones in the conference area. During the conference, attendees will be allowed to dial in to your network by using any of the 15 telephones. Each telephone line has its own telephone number.

The conference attendees can use their own portable computers to dial in. When attendees dial in to TestKingA, they do not need to specify a user name or password. However, you do not want to allow dial-in access from any telephone other than the 15 telephones in the conference area. You enable unauthenticated access on the TestKingA remote access server. You also create a remote access policy named Conference that allows unauthenticated access as the authentication method. Attendees report that they are not able to dial in unless they specify a user name and password. You want to ensure that attendees can dial in without specifying a user name and password. What should you do?

A. Create a user account named Conference Guest. Configure Routing and Remote Access to use the Conference Guest account as the default user identity.
B. Configure the Conference Guest account to use the 15 phone numbers as Caller ID. Create 15 user accounts named Conf-1, Conf-2, Conf-3, and so on through Conf-15. Specify a separate Caller ID phone number for each of the 15 users.
C. Create 15 user accounts that use each phone number as the user name. Configure Routing and Remote Access to use the calling number as the authentication identity.
D. Configure the Conference remote access policy so that it has a Calling-Station ID condition. Use the 15 phone numbers as the condition

Answer: C
Explanation: The calling number can be used for authentication. The remote clients would not need to provide any credentials.
Automatic Number Identification/Calling Line Identification (ANI/CLI) authentication is the authentication of a connection attempt based on the phone number of the caller. The ANI/CLI service returns the number of the caller to the receiver of the call and is provided by most standard telephone companies. In ANI/CLI authentication, a user name and password are not sent.

Incorrect Answers:
A: The user accounts should have the telephone numbers as user names.

B: We want to avoid the need to a supply user name and password. In caller ID authorization, the caller sends a valid user name and password. The caller ID that is configured for the dial-in property on the user account must match the connection attempt; otherwise, the connection attempt is rejected.

D: The calling-station ID condition would allow the calling-station to connect. However, the connecting use still needs to be authenticated and therefore a username and password would still be required.

QUESTION NO: 207
You are the administrator of a Windows 2000 network. Your company wants you to provide a high level of security for its Public Key Infrastructure. You decide to create an offline root Certificate Authority (CA). You want the offline root CA to be capable of processing certificate requests from files, and you want the offline root CA to be recognized as a trusted root authority for Windows 2000 client computers.

How should you create the offline root CA?

A. On a member Windows 2000 Server computer that is connected to the network, create an Enterprise CA. After you install the CA, remove the server to a secure and separate location

B. On a member Windows 2000 Server computer, create a subordinate Enterprise CA that uses a Commercial CA as the certifying authority. After you install the CA, remove the server to a secure and separate location

C. On a stand-alone Windows 2000 Server computer that is isolated from the network, create a stand-alone CA. Export the certificate for the CA to a floppy disk

D. In the Default Domain Group Policy object (GPO), import the certificate to the Enterprise Trust Certificate Store

E. On a stand-alone Windows 2000 Server computer that is isolated from the network, create a stand-alone CA. Export the certificate for the CA to a floppy disk. In the Default Domain Group Policy object (GPO), import the certificate to the Trusted Root Certification Authority Store

Answer: A
Explanation: An offline root CA is used for security reasons to protect it from possible attacks by users on the network. To create an offline root Certificate Authority (CA) we must log on to a Windows 2000 member server that is a part of a domain with a domain administrator's account. While the computer is connected to the network we must install a root CA, not a subordinate CA. The computer must be connected to be able to update the Active Directory, so that its certificates can be used after it has been taken offline. We must then change the URL location of the certificate revocation list (CRL) distribution point to a central location for all users in your organization's network and take the server offline.

Incorrect Answers:
B: The offline CA must be a root CA, not a subordinate CA.
C: The computer on which the offline CA is installed must be a member of the domain, not a standalone server. The computer must also be connected to network when the CA is installed.
D: The CA must be installed on a Windows 2000 member server connected to the network. Just importing a certificate will not work.

E: The CA must be installed on a Windows 2000 member server, not a standalone Windows 2000 server, connected to the network.

QUESTION NO: 208
You are the administrator of a Windows 2000 network. The network consists of one Windows 2000 domain that has Windows 2000 Professional client computers and Windows NT Workstation 4.0 client computers. To create a digital certificate, you use a stand-alone certificate server configured as a root Certificate Authority (CA). You use the digital certificate to secure a virtual directory on your Internet Web server. Users report that when they connect to the virtual directory by means of a new URL, a Security Alert dialog box appears with the following warning message 'The security certificate was issued by a company you have not chosen to trust. You want to prevent this warning message from appearing. You also want to avoid any unnecessary reconfiguration of either the certificate server or the Web server. What should you do?

    A.   Inform your users of the new URL that points to the host name used in the digital certificate.
    B.   Configure a Group Policy that automatically installs as a trusted authority in the client computers the digital certificate for the certificate server.
    C.   Inform your users that they need to install a client certificate from the certificate server.
    D.   Inform your users that they need to install as a trusted authority in the client computers the digital certificate for the certificate server.

Answer: D
Explanation: The server must be viewed as a trusted authority by the clients. They must install a certificate that makes the server a trusted authority for the client, so that they will trust the server. If all clients were Windows 2000 computers the best solution would be to use a Group Policy to deploy the trusted authority certificate, but there are Windows NT 4.0 clients and they cannot use Group Policies. The best solution in this scenario is to inform the users and ask them to install the certificate themselves. After the users have installed a trusted authority in the client computers the digital certificate for the certificate server, they would trust the application server and would not receive any more errors messages like the one given in the scenario above. A certificate is an encrypted set of authentication credentials. A certificate includes a digital signature from the certificate authority that issued the certificate. In the certificate authentication process, your computer presents its certificate to the server, and the server presents its certificate to your computer, enabling mutual authentication. Certificates are authenticated by using a public key to verify this digital signature, which is contained in a trusted authority root certificate that is stored on your computer. These root certificates are the basis for certificate verification and should be supplied only by a system administrator. Windows 2000 provides a number of trusted root certificates. We should add or remove trusted root certificates only if our system administrator advises it.

Incorrect Answers:
A: A trusted authority certificate for the server must be applied on the clients, not a digital certificate that points to the host name of the server.
B: There are Windows NT 4.0 clients and they cannot use Group Policies.

C: A trusted authority certificate, not a client certificate, must be installed.

QUESTION NO: 209
You are the administrator of a Windows 2000 domain. The domain has six Windows 2000 based Routing and Remote Access servers and two Windows 2000 based Internet Authentication Service (IAS) Servers named IAS1and IAS2. The six Routing and Remote access servers use the two IAS servers to authenticate remote access credentials. On IAS1, you change the remote access policies. You want to ensure that this change is also enforced on IAS2.

What should you do?

   A.   In the Active Directory Sites and Services console, force replication from IAS1 to IAS2.
   B.   On IAS1, select **Register service in Active Directory**. Repeat this command on IAS2.
   C.   Use the Netsh command-line utility to copy the IAS configuration from IAS1 to IAS2.
   D.   Manually copy the ras.mdb file from IAS1 to IAS2.

Answer: C
Explanation: Remote Access Policies are not stored in Active Directory; they are stored locally in the IAS.MDB file. To copy the IAS configuration to another server we must type netsh aaaa show config <path>\file.txt at the command prompt. This stores the configuration settings, including registry settings, in a text file. The path can be relative, absolute, or a UNC path. We must then copy the file we created to the destination computer, and at a command prompt on the destination computer, type netsh exec <path>\file.txt. A message will appear indicating whether the update was successful or not.

Incorrect Answers:
A: Remote Access Policies are not stored in Active Directory; they are stored locally in the IAS.MDB file.
B: Remote Access Policies are not stored in Active Directory.
D: There is no such a thing as a ras.mdb file in Windows 2000.

QUESTION NO: 210
You are the administrator of TestKing's network, which consists of a vendor subnet and several internal subnets. Two servers, VPN1 and Router1, run Windows 2000 Server and Routing and Remote Access. Each server contains two network adapters named NIC1 and NIC2. Company users need to access both internal and external network resources every business day.

The vendor subnet is used by several vendors contracted by your company. Two of these vendors now need to access HTTP resource on your internal subnets. Their client computers run Windows 2000 Professional. For security reasons, you require these two vendors to access VPN1 by creating a virtual private network (VPN) connection that uses an L2TP/IPSec tunnel.

To reduce network traffic through VPN1, you want to prevent the two vendors from using the VPN connection to access Internet resource. You decide to configure a TCP/IP filter on one of your network adapters to drop HTTP traffic originating from the Vendor subnet.
Which network adapter should you reconfigure?

Answer by clicking the appropriate network adapter in the network diagram.
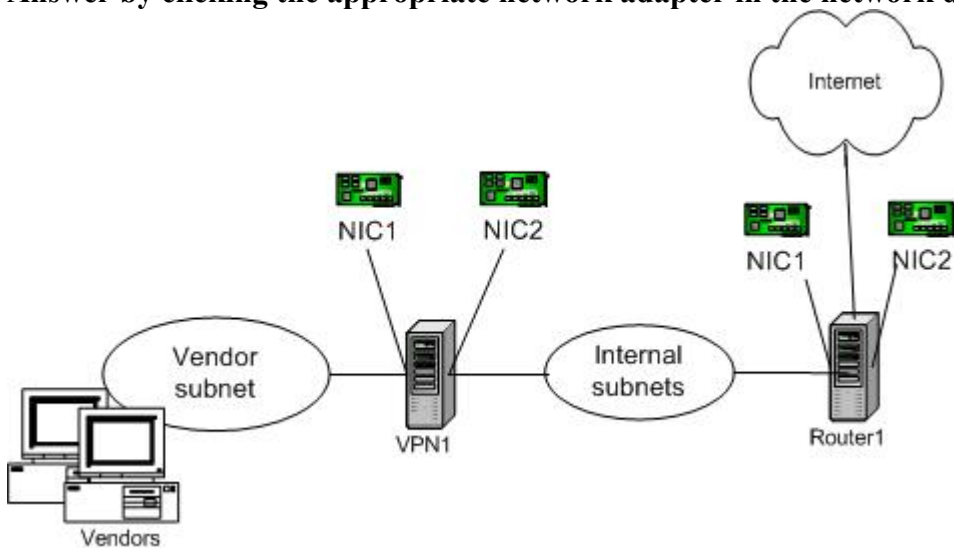
Answer:
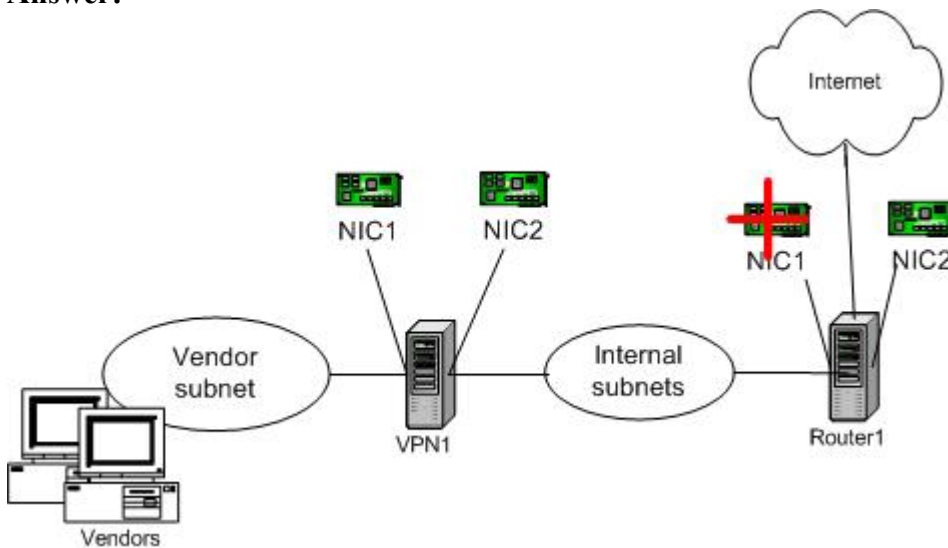
Explanation: We configure a TCP/IP filter on NIC1 on Router1 to drop HTTP traffic originating from the Vendor subnet. This way the HTTP vendor traffic will never get through Router1 and the vendors will not be able to reach the Internet through HTTP.

Incorrect answers:
NIC1 VPN1
If we trop HTTP traffic on NIC1 on the VPN1 server the vendors cannot use HTTP resources on the Internal subnets.
NIC2 VPN1
If we trop HTTP traffic on NIC2 on the VPN1 server the vendors cannot use HTTP resources on the Internal subnets.
NIC2 Router1
We should put the TCP/IP filter on the internal interface, NIC1, on Router1, not the external interface NIC2. It is unnecessary to let the vendor HTTP traffic reach NIC2. It would increase the load on Router1.

QUESTION NO: 211
You are the administrator of TestKing's network, which consists of a single Windows 2000 Domain. The relevant portion of its configuration is shown in the exhibit.
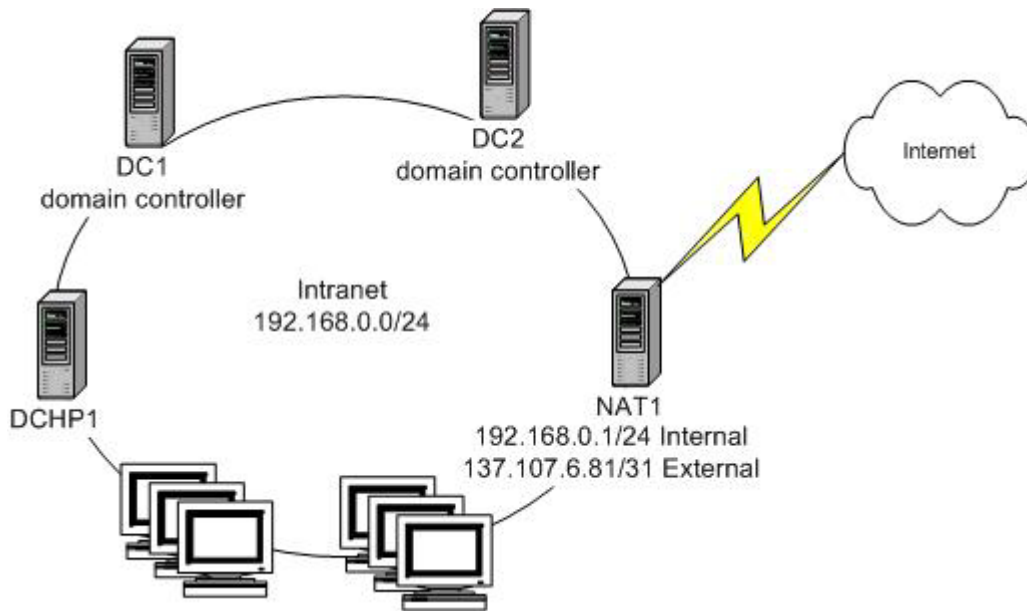
You configure a Windows 2000 Server computer named NAT1 as the DNS server for the domain. You install Routing and Remote Access on NAT1. You configure NAT1 to provide network address translation services for client computers to access the Internet.

Users now report that they cannot log on to the domain or access network resources. On investigation, you discover that you cannot query NAT1 for name resolution. In the application event log on NAT1, you find the following event messages:

```
Event ID: 407
Source: DNS
Description: DNS server could not bind a datagram (UDP) socket to
192.168.0.1. The data is the error.

Event ID: 408
Source: DNS
Description: DNS server could not open socket for address 192.168.0.1.
Verify that this is a valid IP address on this machine.
```

How should you correct this problem?

A.   Disable the DNS proxy functionality on NAT1
B.   Enable the DNS proxy functionality on NAT1
C.   Reconfigure the DNS server service not to listen on the internal address of NAT1.
D.   Reconfigure the DNS server service not to listen on the external address of NAT1.

Answer: C

Explanation: This problem can occur when you have a NAT server that also is used as a DNS server. NAT has a DNS Proxy setting that enables DHCP clients to direct DNS queries to the NAT server. The client DNS queries are then forwarded to the NAT server's configured DNS server. The DNS Proxy and the DNS Server service cannot coexist on the same host, if the host is using the same interface and IP address with the default settings.

There are three methods to overcome this problem:
1. Reconfigure the DNS server service not to listen on the internal address. This is the solution in this scenario.
2. Install NAT and DNS on different servers. We cannot change this configuration here since this option is not listed.
3. Use the DHCP server Service in NAT, NOT the DHCP Allocator and DNS Proxy.

Reference: JSI Tip 3284, Your DNS Event Log reports Event Ids 407 and 408

Incorrect Answers:
A: We could disable both the DNS proxy functionality and the DHCP allocator.
B: The DNS proxy function on the NAT server is partly to blame. Enabling it will not help.
D: We must configure the DNS server not to listen to the internal address, not the external address.

QUESTION NO: 212
You are the network administrator for your company. You plan to create a fully routed network. You configure three Windows 2000 Server computers as RIP routers, as shown in the following diagram:
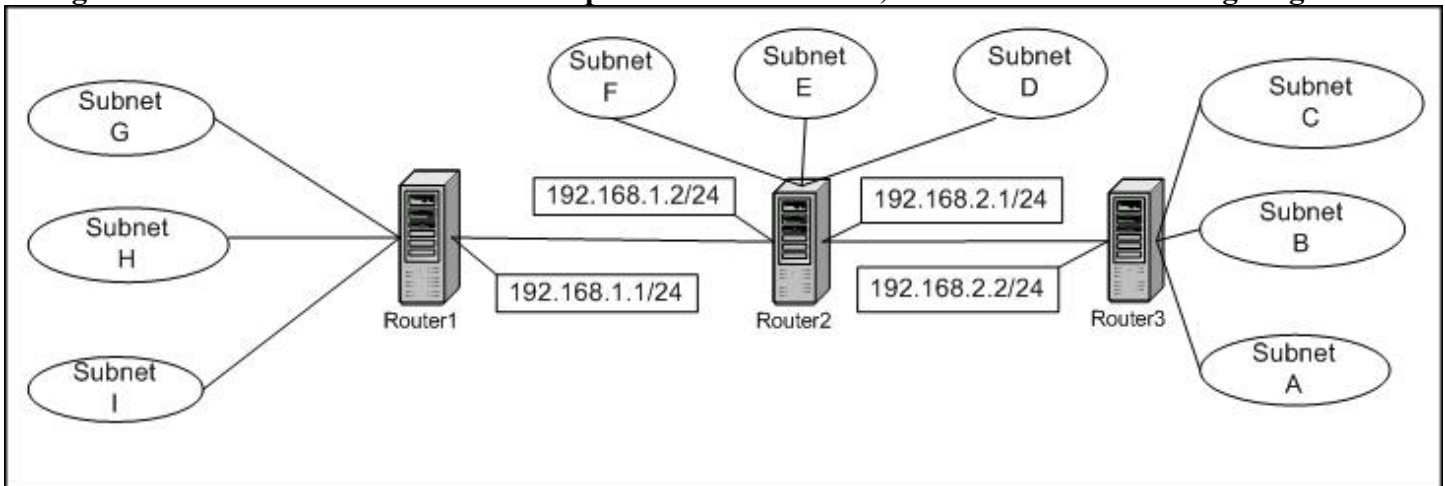
Your configuration is intended to ensure that RIP traffic is received only by the RIP routers. However, you discover that RIP traffic from Router2 is being received by hosts other than the RIP routers. In addition, users in Subnet A report that they cannot communicate with a database on Subnet D.
You open the RIP properties dialog box for Router2. The relevant portion of the dialog box is shown in the exhibit.

Leading the way in IT testing and certification tools, www.testking.com
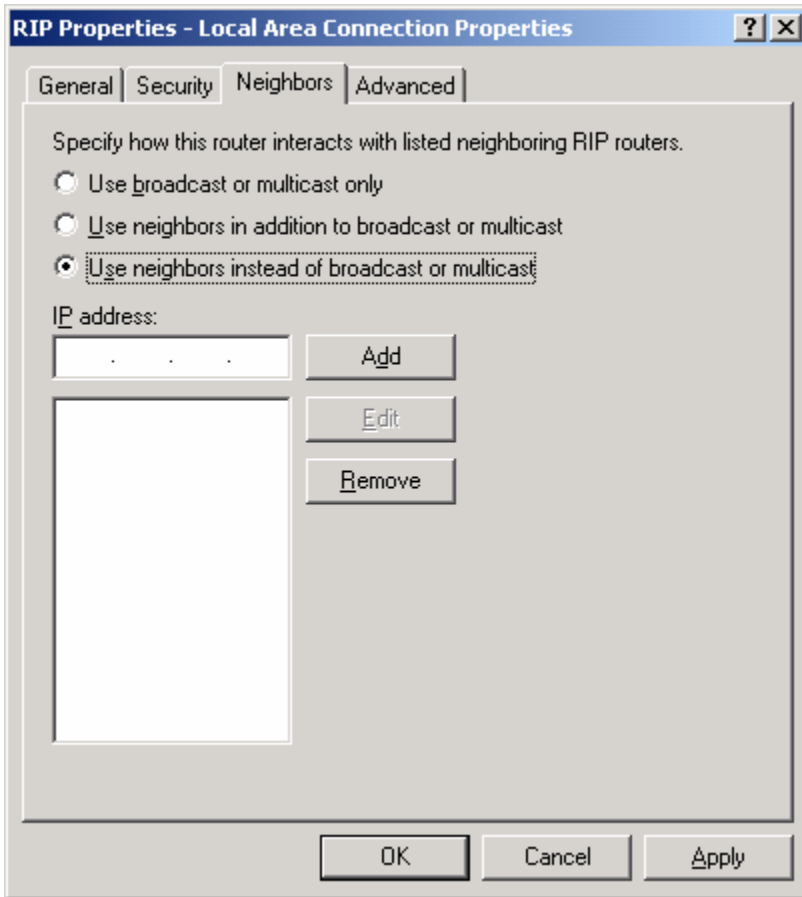
You need to correct this problem by reconfiguring the RIP properties on Router2. Your solution must involve the least possible administrative effort.
What should you do?

    A.   Remove the IP address 192.168.1.1 and add the IP address 192.168.1.2 to the Properties page for RIP neighbors on the 192.168.2.1 interface.
    B.   Remove the IP address 192.168.2.1 and add the IP address 192.168.2.2 to the Properties page for RIP neighbors on the 192.168.2.1 interface.
    C.   Remove the IP address 192.168.2.1 and add the IP address 192.168.1.2 to the Properties page for RIP neighbors on the 192.168.1.2 interface.
    D.   Remove the IP address 192.168.1.1 and add the IP address 192.168.2.2 to the Properties page for RIP neighbors on the 192.168.1.2 interface.

Answer: B
Explanation: The exhibit shows that RIP is configured for neighbors instead of broadcasts. There is a communication problem between the subnets A and D. We must add the appropriate RIP neighbor on Router2. We add the Interface on Router3, IP address 192.168.2.2, on the 192.168.2.1 interface on Router2.

In addition we remove the interface address itself from the interface. This helps to prevent other hosts from receiving RIP traffic.

Note: By default, RIP either broadcasts (RIP version 1 or RIP version 2) or multicasts (RIP v2 only) announcements. To prevent RIP traffic from being received by any node except neighboring RIP routers, the Windows 2000 router can unicast RIP announcements.

Incorrect Answers:
A: The IP address 192.168.1.1 should not be present as a neighbor on the 192.168.2.1 interface on Router2. Removing it would not solve any problems however. Instead we should remove 192.168.2.1 from the 192.168.2.1 interface.
C: We must reconfigure the 192.168.2.1 interface, not the 192.168.1.2 interface, on Router2. The 192.168.2.1 interface connects subnet A and subnet D.
D: We must reconfigure the 192.168.2.1 interface, not the 192.168.1.2 interface, on Router2. The 192.168.2.1 interface connects subnet A and subnet D.

QUESTION NO: 213
You are the administrator of TestKing's network, which includes one Windows 2000 Domain in native mode. Four servers on the network are available for remote users. All four member servers are running Windows 2000 Server and Routing and remote access. Currently, remote access is administered individually by Active Directory user attributes.
You administer remote access by using centralized remote access policies. Which courses of action should you perform? (Each correct answer presents part of the solution. Choose two)

    A.   Configure the four servers as RADIUS clients
    B.   Configure the four servers as domain controllers in the existing domain
    C.   Configure the four servers as domain controllers in a new domain in a separate forest. On a Windows 2000 member server in the new domain, configure the Internet authentication service (IAS). Create a remote access policy on the IAS server.
    D.   Configure the four servers as domain controllers in a new domain in a separate forest. On a Windows 2000 member server in the new domain, configure the Internet authentication service (IAS). Create a remote access policy on a domain controller to administer all remote access users.
    E.   On a Windows 2000 member server in the existing domain, configure the Internet authentication service (IAS). Create a remote access policy on a domain controller to administer all remote access users.
    F.   On a Windows 2000 member server in the existing domain, configure the Internet authentication service (IAS). Create a remote access policy on the IAS server

Answer: A, F
Explanation: IAS is Microsoft's implementation of a RADIUS server and is used to centralize administration of RRAS servers.
A: The RRAS servers are set up as RADIUS clients.

F: We configure the central remote access computer, the IAS server, on a Windows 2000 member server and one remote access policy on it that will be used by all the RADIUS clients.

Reference: Microsoft White paper, Internet Authentication Service for Windows 2000

Incorrect Answers:
B: The four servers should be configured as RADIUS clients, not domain controllers.
C: There is no need for the RADIUS clients to be domain controllers. On the contrary it could endanger security.
D: There is no need for the RADIUS clients to be domain controllers. On the contrary it could endanger security.
E: The remote access policy should be placed on the IAS server, not on a domain controller.

QUESTION NO: 214
You are the network administrator for TestKing. The network consists of a single Windows 2000 Domain with three sites, as shown in the exhibit.
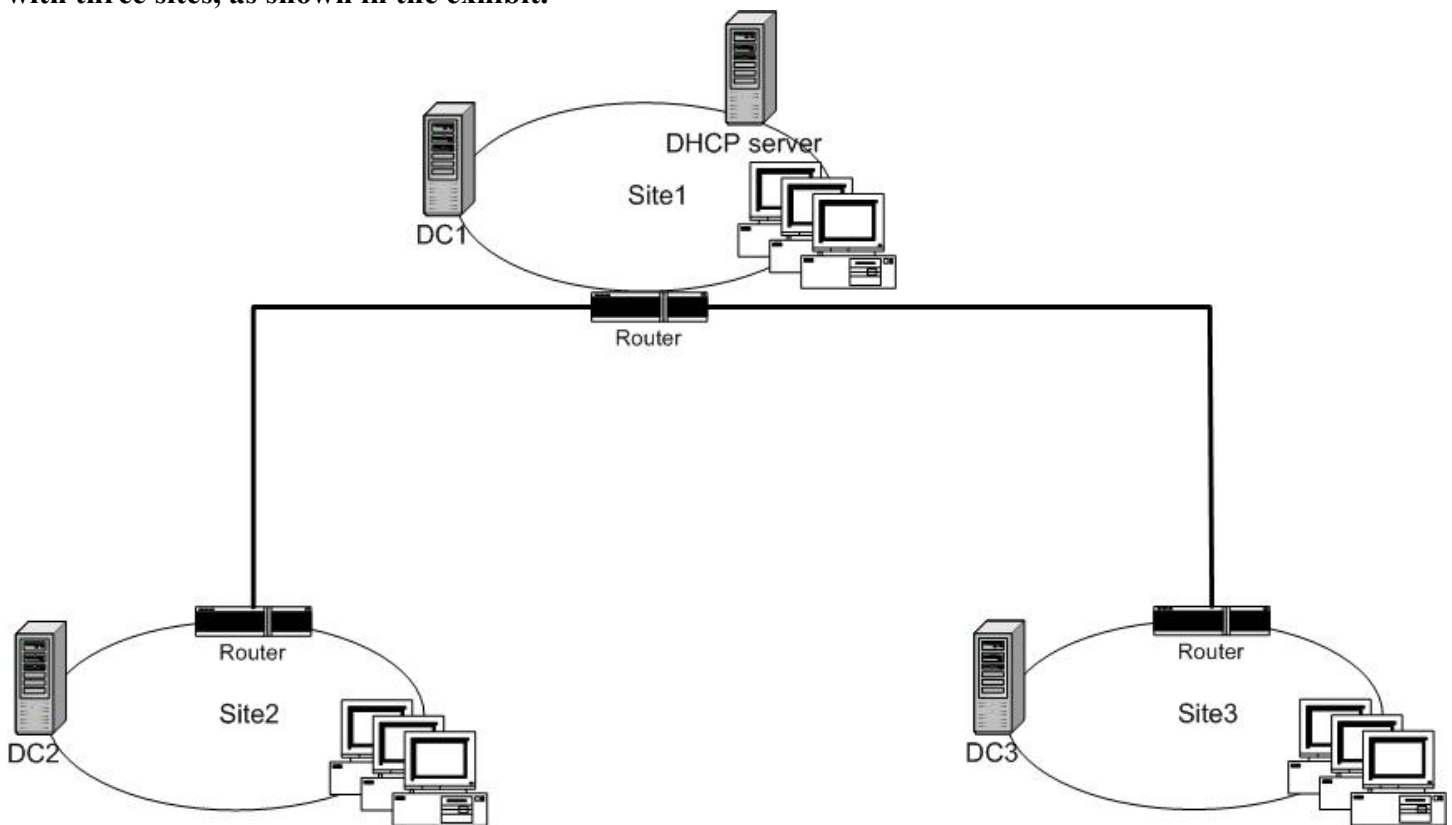
Users in Site3 report they cannot log on to the domain or access any resources in the other sites.
You check a client computer. It has an IP address of 169.254.13.74.
What should you do?

A. Disable Automatic Private IP Addressing (APIPA) on the client computers

B. Add a new scope to the DHCP server for the computers in Site3

C. Configure a DHCP Relay Agent on DC3

D. Add reservations in the DHCP scope for all client computers

Answer: C
Explanation: The clients on Site3 are unable to communicate with the DHCP server. They are configured with APIPA address instead. By installing a DHCP Relay agent in the subnet of Site3 the clients will be able to receive IP configuration from the DHCP server.

Incorrect answers:
A: Disabling APIPA on the client computers will not help them receive IP configuration from the DHCP server. They would have no IP configuration at all.
B: Any configuration of the DHCP server will not help. The clients are unable to receive IP configuration from the DHCP server.
D: Any configuration of the DHCP server will not help. The clients are unable to receive IP configuration from the DHCP server.

QUESTION NO: 215
You are the administrator of TestKing's network, which consists of five servers running Windows 2000 Server and 20 client computers running Windows 2000 Professional.
All Servers have static IP address and all client computers use Automatic Private IP Addressing (APIPA) for IP address assignment. One server is multihomed, with a persistent connection to TestKing's Internet service provider (ISP).

Your company is acquired by another company. You must provide Internet access for all internal users. You must also enable remote users to access your internal servers. Your solution must involve the fewest possible changes to your current network configuration.

Which action or actions should you perform? (Choose all that apply.)¨

A. Enable Internet Connection Sharing on the multihomed server.

B. Install the Network Address Translation protocol (NAT) on the multihomed server.

C. Configure the multihomed server as a DHCP allocator and exclude the static server addresses.

D. Map the internal server addresses and ports to IP addresses in a pool assigned by your ISP.

E. Configure the external interface on the multihomed server as a demand-dial interface for DNS query resolution.

Answer: B, C, D
Explanation:
There are basically three ways to provide Internet access in a Windows 2000 network: ICS, NAT, and Proxy server. NAT is the appropriate solution in this scenario.
B: NAT must be installed on the multihomed server.
C: The clients are currently using private APIPA addresses. They cannot use access Internet with APIPA addresses. Instead we configure the DHCP allocator on the NAT computer.
D: We provide remote access through Internet with mapping public IP addresses to ports and internal addresses.

Incorrect answers:
A: To enable external users to access internal resources, we need static mappings of external IP addresses to ports and internal IP addresses. You cannot do this with ICS; you can only do this with NAT.
E: There is a persistent connection, not a dial-up connection, to the ISP. There is no need of a demand-dial interface.

QUESTION NO: 216
You are the network administrator for TestKing. The network consists of five domains in four locations, as shown in the exhibit.
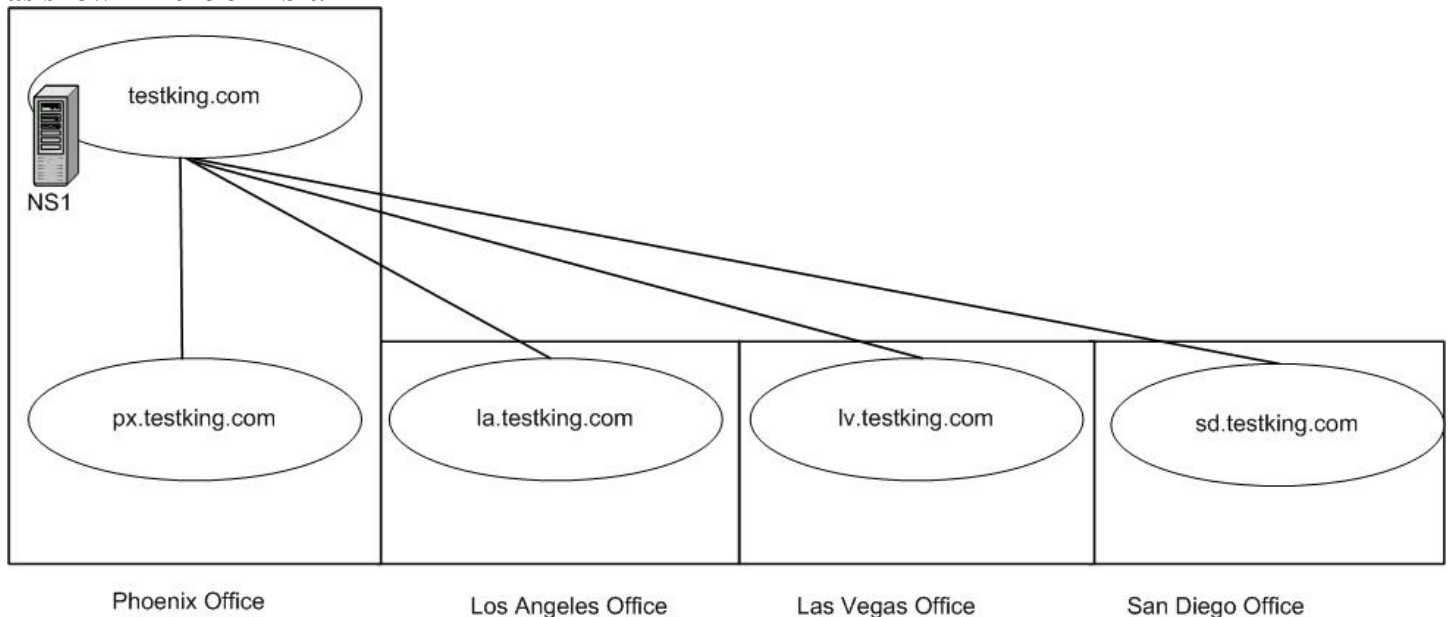
The branch offices in Los Angeles, Las Vegas, and San Diego are connected to the main office in Phoenix by means of 640-KB lines.

You install a DNS server named ns1.testking.com at the main office. It hosts the zones shown in the following table.

Zone	Zone Type	Allows dynamic updates?
testking.com	Standard primary	Yes
px.testking.com	Standard primary	Yes
la.testking.com	Standard primary	Yes
lv.testking.com	Standard primary	Yes
sd.testking.com	Standard primary	Yes

Users need to improve network response times for users and reduce traffic over the WAN links. To do so, you install the DNS service on a domain controller in each branch office.

What should you do next?

A. Move the zone files for each primary zone to the appropriate local server.
Configure the DNS servers in the branch offices to forward unresolved requests to ns1.testking.com.
Configure the client computers in the branch offices to use the address of their local DNS server.

B. Delete the location-specific primary zones from ns1.testking.com and re-create them as subdomains of the testking.com zone.
Create secondary zones on the DNS servers in the branch offices and use the subdomains as the master zones.
Configure the client computers in the branch offices to use the address of their local DNS server.
Configure the DNS servers in the branch offices to forward unresolved requests to ns1.testking.com

C. On each DNS server in the branch offices, create an Active Directory integrated zone for the local domain only.
Convert the location-specific primary zones on ns1.testking.com to secondary zones that use the Active Directory zones as the master zones.
Configure the client computers in the branch offices to use the address of their local DNS Server.
Configure the DNS servers in the branch offices to forward unresolved requests to ns1.testking.com

D. Configure the DNS servers in the branch offices as caching-only servers.
Convert all primary zones on ns1.testking.com to Active Directory integrated zones.
Configure the caching-only servers to forward unresolved requests to ns1.testking.com.
Configure the client computers in the branch offices to use the address of their local DNS server.

Answer: C
Explanation: By creating Active Directory integrated zones in the local offices local name resolution would not involve the main office. This saves bandwidth and improves performance. By using secondary zones for each local zone at the main office, local name resolution can be performed from the main office. We also configure the local DNS server to forward non-local name resolution to the central DNS server.

Incorrect Answers:
A: We cannot have primary zones both in the main office and in the four locations.

Leading the way in IT testing and certification tools, www.testking.com

B: Creating secondary zones at the locations will reduce name resolution traffic. But secondary zones are read-only so all updates in all zones must be made at the main office. It would be better to make updates to the zones locally.

D: Caching-only servers are usable on slow WAN links. A 648Kbps WAN link cannot be considered slow. A WAN link of 128Kbps or less is considered a slow WAN link.

QUESTION NO: 217
You are the network administrator for Contoso Ltd. Your network consists of a single Windows 2000 domain and a single standard primary DNS zone. The network includes four domain controllers: D-DC1, D-DC2, S-DC, and B-DC. The relevant portion of its configuration is shown in the exhibit.
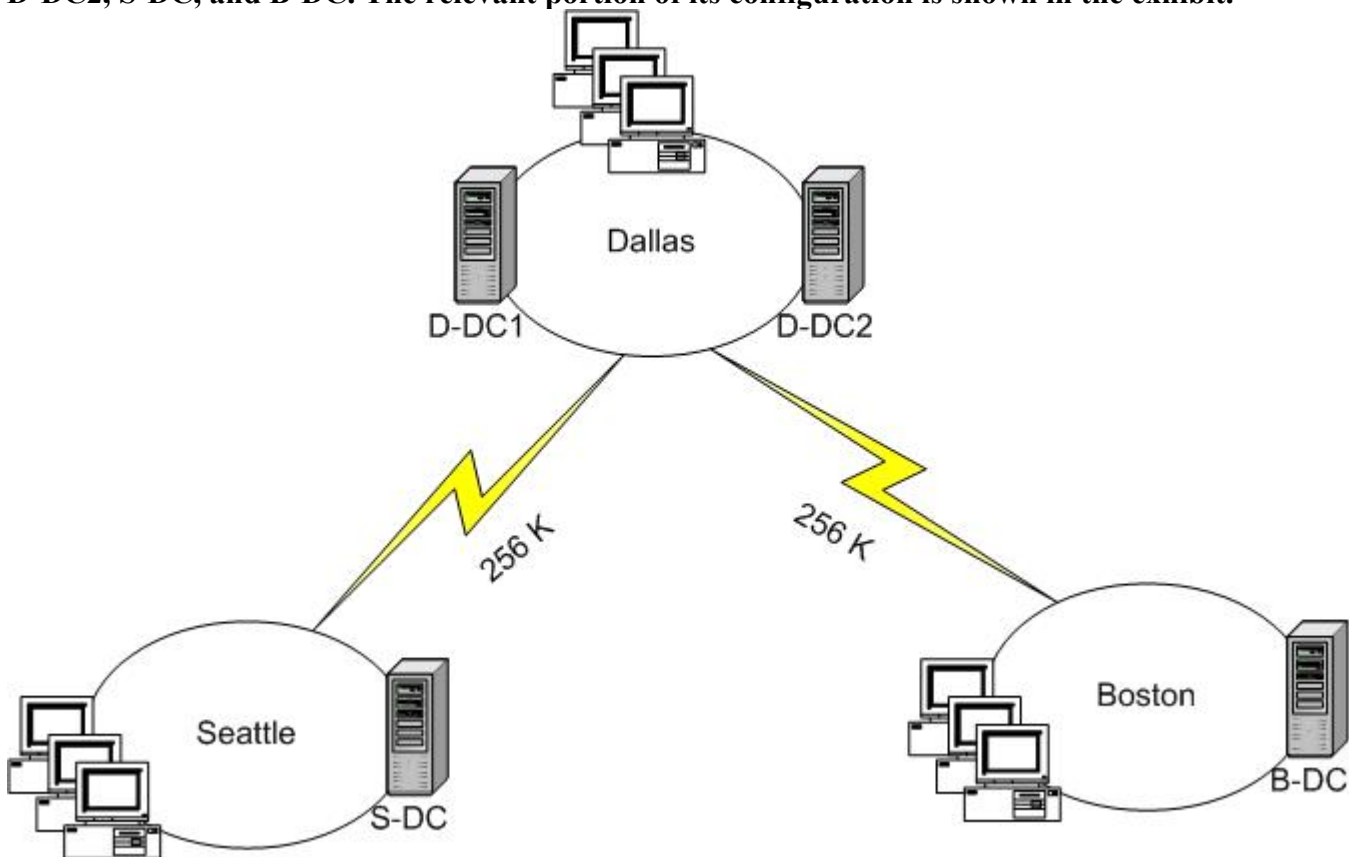
Users in the Seattle and Boston offices report that response times are extremely slow when they try to log on to the domain to access intranet resources. On investigation, you discover that DNS name resolution queries are generating heavy traffic across the WAN links.

You need to improve network response times for users and reduce name resolution traffic between the offices. To do so, you place one new member server in Seattle and another in Boston. You install the DNS Server service on both servers.

What should you do next?

A. Create an Active Directory integrated zone on each new server.
   Convert the existing zone to an Active Directory integrated zone.
   Configure the client computers in each office to query their local DNS server.

B. Create a standard primary zone on each new server.
   Add resources records for each office's intranet resources to the zone.
   Configure the client computers in each office to query their local DNS server.

C. Create a standard secondary zone on each new server.
   Use the primary zone at the main office as the master zone.
   Configure the client computers in each office to query their local DNS server.

D. Create a standard primary zone on each new server.
   Configure the servers to forward requests to the DNS servers in the main office.
   Configure the client computers in each office to query their local DNS server.

Answer: C
Explanation: We should create standard secondary zones on the new member servers in Seattle and Boston.
They should be configured to use the primary zone at the main office in Dallas as the master zone. Finally the
client computers in Seattle and Boston should be configured to query their local DNS server.
This would improve network response times and reduce name resolution on the WAN links.

Incorrect Answers:
A:　　We cannot use Active Directory integrated zones on the member Servers in Seattle and Boston. Active
　　　　Directory zones require domain controllers.
B:　　We cannot use primary zones both at Dallas and at the local offices Boston and Seattle.
D:　　We cannot use primary zones both at Dallas and at the local offices Boston and Seattle.

QUESTION NO: 218
You are the administrator of TestKing's network, which includes 100 computers running Windows 2000
Professional and 10 computers running Windows 2000 Server. All client computers are DHCP clients. All
servers have static IP addresses.

Your company plans to use network address translation to provide Internet access for all client
computers on the network. In addition, both internal and remote users must be able to access internal
servers. Because you anticipate growth in the near future, you lease a pool of 100 addresses from an
Internet service provider (ISP).

You configure the Network Address Translation protocol (NAT) on a server named NATSvr1, which has
a persistent connection to the ISP. You map the ports and addresses of your internal servers to ports and
addresses in the pool assigned by the ISP.

Ten internal users now report that they have no Internet access. However, these users can access internal network resources. Remote users can access all internal from the Internet.

You must enable all internal users to access the Internet. You must continue to enable all remote users to access internal network resources.

What should you do?

    A.   Remove the existing DHCP server and enable the DHCP allocator on NATSvr1.

    B.   From your internal servers, remove the port and address mappings to the ports and addresses in the pool assigned by the ISP.

    C.   Enable the translation of TCP/UDP headers for the public interface for NAT.

    D.   Map the IP addresses of the client computers without Internet access to IP addresses in the pool assigned by the ISP.

Answer: A

Explanation: We must use the DHCP allocator that is included in NAT, to provide IP addresses to the clients.

Incorrect Answers:
B: The mapping of the IP addresses leased from the ISP to internal IP addresses and ports, provides external users with access to the local network.
C: There is no need to enable NAT translation to provide Internet access.
D: Mappings are used to provide external users access to internal resources. Mappings will not provide internal users with Internet access.

QUESTION NO: 219
You are the network administrator for Blue Yonder Airlines. Your network includes 300 client computers and 10 servers. All client computers run Windows 2000 Professional and use DHCP for IP address assignment. Eight servers run Windows 2000 Server and two servers run Windows NT Server 4.0. One Windows 2000 Server computer functions as your internal Web server. All servers have static IP addresses.

You plan to provide Internet access for all your client computers by using the Network Address Translation protocol (NAT). You also want to enable both internal and remote users to access internal servers.

You lease a pool of 50 IP addresses from an Internet service provider (ISP). You install and configure NAT on a Windows 2000 Server computer named NATSvr1. This computer has a persistent connection

to the ISP. The relevant portion of the resulting network configuration is shown in the exhibit.
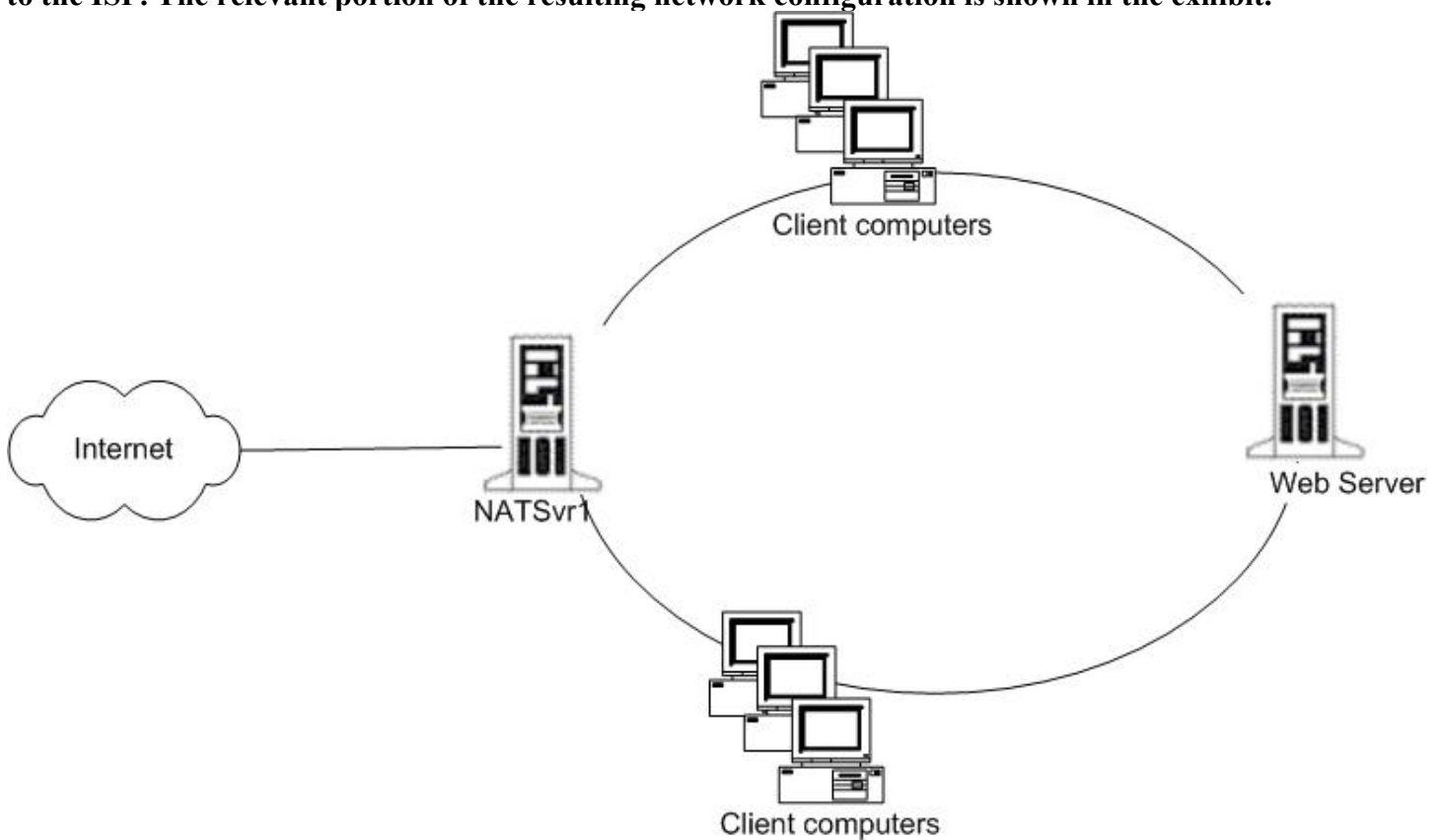
Now you need to enable remote users to access your internal Web server.
Your solution must involve the least possible administrative effort.

What should you do?

A.   On NATSvr1, select the Clients using Domain Name System (DNS) check box.

B.   Map your Web server's internal address and port to an address and port in the pool leased from the
ISP.

C.   Install and configure an internal DNS server for your network. Configure all remote users to use this
computer as their DNS server.

D.   From the pool leased from the ISP, reserve 10 IP addresses for use by internal servers.

Answer: B
Explanation: Access to internal resources for external users on the Internet is provided with mappings from
public leased IP address to local addresses and ports. In this scenario we map the Web server's internal address
and port to a leased IP address.

Reference: HOW TO: Configure a Windows 2000 Server as a Network Address Translation Server (Q299801)

Incorrect Answers:
A: The **Clients using Domain Name System (DNS)** setting is a configuration that sets up NAT. It is not specifically used enable the access of internal resources through the Internet.
C: There is no requirement to use DNS when NAT is used.
D: The leased addresses are used to create mappings. These addresses don't have to be used by the internal clients.

QUESTION NO: 220
You are the administrator of TestKing's network, which includes personal computers and one mainframe computer. You divide the network into two LANs. One LAN contains the personal computers, and the other contains the mainframe computer. The relevant portion of the resulting configuration is shown in the exhibit.
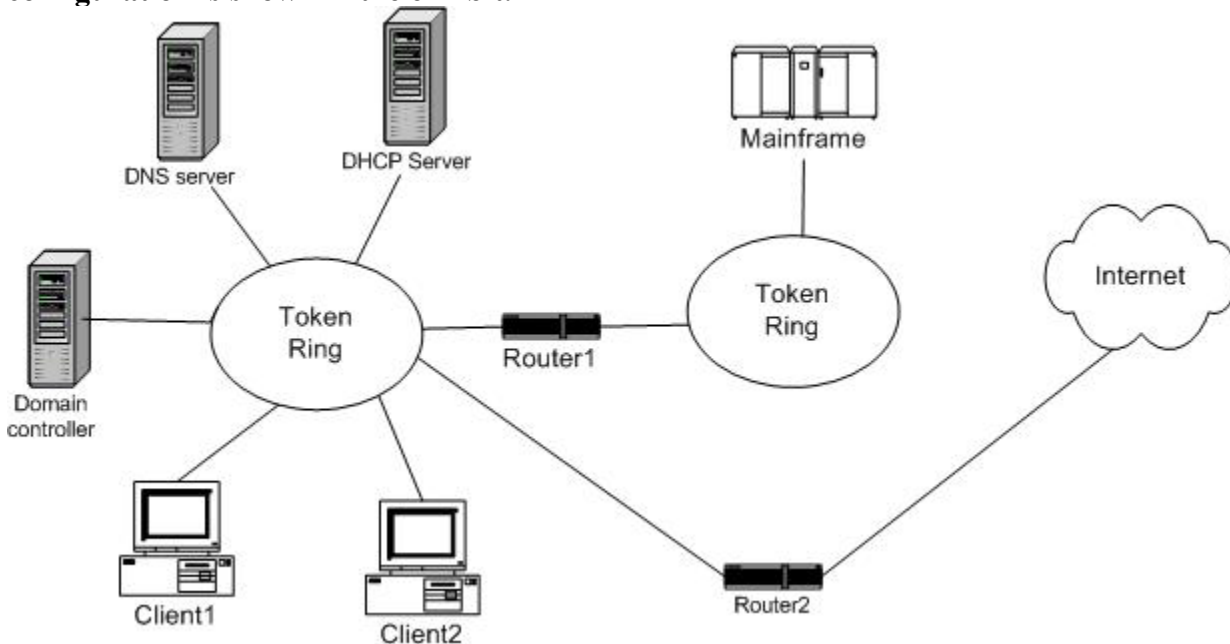
TCP/IP is the only transport protocol in use on both LANs. All client computers are DHCP clients, and all use third-party TN3270 client software to connect to the mainframe computer.

Users now report that they cannot access resources located on the mainframe computer, either by using its host name or by using its IP address. They report no problems accessing Internet resources.

You need to ensure that client computers can access resources on the mainframe computer without affecting Internet connectivity. Your solution must involve the least possible administrative effort.

What should you do?

A.   Install the DLC protocol on each client computer.
B.   Configure an SNA gateway on the personal computer-based LAN.
C.   Implement source-route bridging on Router1.
D.   Configure the DHCP Static Route option to specify the route to the mainframe computer.
E.   Configure the DNS server with an A (host) record for the mainframe computer.

Answer: D
Explanation: This is a TCP/IP problem, not a DNS or software compatibility problem. The clients must be able to use a static route to access the mainframe. This configuration can be included in the DHCP scope options.

Incorrect Answers:
A: The DLC protocol cannot be routed. It would not be useful to install it on the clients.
B: A SNA gateway would not be needed since the clients already are running client software that enables communication with the mainframe.
C: Source bridge routing is used in networks containing bridges. There are no bridges in this network.
E: This is not a DNS problem, since the mainframe cannot be access by IP address either.

QUESTION NO: 221
You are the administrator of TestKing's network, which is divided into 50 segments. Segments 1 through 5 are connected to the Internet. All segments are connected by routers. The network also includes one DHCP server.

Your company purchases an online training software package that uses multicast video. The software package will be installed on a dedicated video server located on Segment 1. The video server will deliver training videos to client computers located on the same segment.

You must ensure that your DHCP server can issue multicast IP addresses. You must also ensure that the multicast video cannot be received by client computers located on other segments or by external computers on the Internet.

You plan to create a multicast scope. For which subnet should you create the multicast scope?

A.   224.0.0.0/4
B.   224.0.0.0/8
C.   224.0.0.0/14
D.   224.0.0.0/24

Answer: D
Explanation: Multicast is a scheme for using IP addresses 224.0.0.0 through 239.255.255.255 to send the same data to several machines simultaneously.

Multicast boundaries are configurable administrative barriers that limit the extent of the IP internetwork over which multicast traffic can be forwarded. Without boundaries, an IP multicast router forwards all appropriate IP multicast traffic. Scope-based boundaries prevents the forwarding of IP multicast traffic with a specified group IP address or range of IP addresses.

The range 224.0.0.0 through 224.0.0.255 is reserved for local purposes (as administrative and maintenance tasks) and datagrams destined to them are never forwarded by multicast routers. This is the 224.0.0.0/24 network.

Reference:
RFC2365
Multicast over TCP/IP HOWTO
What Is IP Multicast? (Q165011)

Incorrect Answers:
A, B, C: These networks would forward multicasts outside the local network.

QUESTION NO: 222
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The network has a persistent connection to the Internet. The relevant partition of its configuration is shown in the exhibit.

Your company employs mobile salespeople who use portable computers running Windows 98. To enable these users to access internal resources you place a virtual private network (VPN) server named VPN1 outside your firewall. This server is a stand-alone Windows 2000 Server computer running Routing and Remote Access. The firewall is configured to allow inbound access from VPN1 only.

Leading the way in IT testing and certification tools, www.testking.com

You configure PPTP ports on VPN1. Now you must configure packet filters. VPN1 must allow only VPN traffic on the Internet interface and it must prevent non-VPN users from accessing internal resources.

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

A. Using the PPTP ports as the destination ports, create an input filter on VPN1.
As the destination IP address, use the IP address of the external interface of VPN1.
B. Using the PPTP ports as the source ports, create an input filter on VPN1.
As the source IP address, use the IP address of the external interface of VPN1.
C. Using the PPTP ports as the destination ports, create an input filter on VPN1.
As the destination IP address, use the IP address of the internal interface of VPN1.
D. Using the PPTP ports as the source ports, create an output filter on VPN1.
As the source IP address, use the IP address of the external interface of VPN1.
E. Using the PPTP ports as the destination ports, create an output filter on VPN1.
As the destination IP address, use the IP address of the external interface of VPN1.
F. Using the PPTP ports as the source ports, create an output filter on VPN1.
As the source IP address, use the IP address of the internal interface of VPN1.

Answer: A, F
Explanation:
A: The only inbound traffic allowed is traffic to the external interface on the VPN1 server.
F: The only outbound traffic allowed is traffic originating from the internal interface of VPN1.

Incorrect Answers:
B: Input filters must use the PPTP ports as destination ports.
C: The only destination address allowed is the address of the external VPN interface.
D: The source of an output filter must the IP address of the internal interface of VPN1.
E: In an output filter the PPTP ports must be used as a source ports.

QUESTION NO: 223
You are the administrator of TestKing's network. All computers on the network run Windows 2000. Two servers named ServerA and ServerB support a confidential medical records database. ServerA runs the database and ServerB runs a middle-tier application that employees use to access the database.

Your company decides to implement IPSec policies to increase network security. To ensure that all communications on ServerA are secure and encrypted, and to ensure that only ServerB can access resources on ServerA, you assign the default Secure Server IPSec policy on both ServerA and ServerB.

However, users report they can no longer access ServerB. How should you correct this problem?

A. Change the authentication header (AH) algorithm on ServerB to MD5.

B.   Change the encapsulating security payload (ESP) protocol algorithm on ServerB to DES.
C.   Assign a custom IPSec policy on ServerA. This policy will require IPSec authentication headers
        (AH) and the encapsulating security payload (ESP) protocol for traffic that originates from the IP
        address of ServerB.
D.   Assign the Client (Respond Only) IPSec policy on Server B.

Answer: D
Explanation: We need to ensure that all communications to and from ServerA are encrypted. We can
accomplish this by applying the default Secure Server IPSec policy on ServerA. In this scenario we have also
applied this policy at ServerB. This enforces encryption on all communication on ServerB as well, and this is
the reason that ServerB is no longer accessible to the clients (the clients haven't been configured for IPSec).
There is no requirement that all traffic to and from ServerB should be encrypted. We should change the IPSec
policy to Client (Respond only). This enables non-encrypted communication with ServerB, and ServerA would
still be secure.

Incorrect Answers:
A: We should change the IPSec policy, not the AH configuration on ServerB.
B: We should change the IPSec policy, not the ESP configuration on Server B.
C: There is no need to change the IPSec policy on ServerA. It must be changed on ServerB.

Q.224
**You are the network administrator for a small company. Your network consists of three subnets named
A through C and a connection to the Internet. These subnets are connected by three Windows 2000
Server computers, which are configured as network routers in a default configuration, as shown in the
exhibit.**
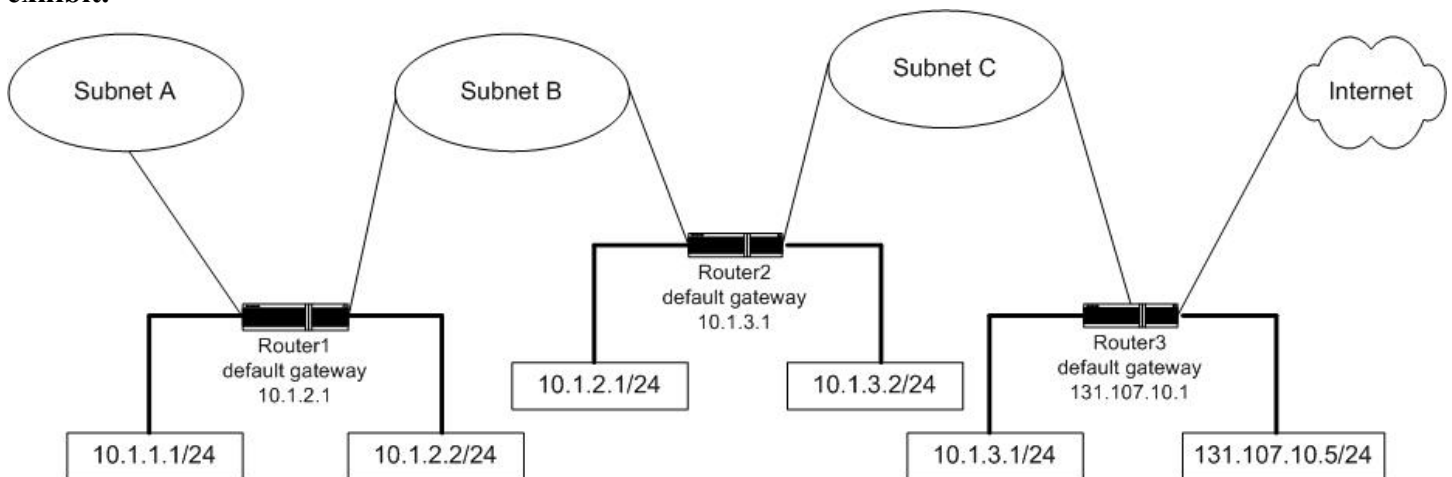
**To enable all hosts on all subnets to communicate with each other, you need to add static route entries on
your routers. Which three entries should you add? (Choose three.)**

Leading the way in IT testing and certification tools, www.testking.com

A.   for the 10.1.3.0/24 subnet on Router1
B.   for the 10.1.4.0/24 subnet on Router1
C.   for the 10.1.1.0/24 subnet on Router2
D.   for the 10.1.4.0/24 subnet on Router2
E.   for the 10.1.1.0/24 subnet on Router3
F.   for the 10.1.2.0/24 subnet on Router3

Answer: C, E, F.
Explanation:
C: Router2's default gateway is Router3. Whenever Router2 receives a packet destined for the 10.1.1.0/24 subnet, it will send the packet to Router3 because Router2 doesn't know how to get to 10.1.1.0/24. We must therefore add a static route for 10.1.1.0/24 on Router2.
E: Router3's default gateway is a router on the internet. Whenever Router3 receives a packet destined for the 10.1.1.0/24 subnet, it will send the packet to the router on the internet (the default gateway) because Router3 doesn't know how to get to 10.1.1.0/24. We must therefore add a static route for 10.1.1.0/24 on Router3.
F: Router3's default gateway is a router on the internet. Whenever Router3 receives a packet destined for the 10.1.2.0/24 subnet, it will send the packet to the router on the internet (the default gateway) because Router3 doesn't know how to get to 10.1.2.0/24. We must therefore add a static route for 10.1.2.0/24 on Router3.

Incorrect Answers:
A: Router1 can get to 10.1.3.0/24 because Router1's default gateway is Router2 which is directly connected to 10.1.3.0/24.
B: There is no 10.1.4.0/24 subnet in the network
D: There is no 10.1.4.0/24 subnet in the network

QUESTION NO: 225
You are the administrator of TestKing's network, which consists of a single site. The network contains 3,000 computers running Windows 2000 Professional and 100 computers running Windows 2000 Server. One server runs WINS.

Your company acquires a subsidiary with a large network environment. The subsidiary's network links one main office and four branch offices. The main office has two WINS servers, and each branch office has one WINS server. Their routers do not support the Internet Group Messaging Protocol (IGMP).

You want to integrate your existing WINS server with the WINS servers on the subsidiary's network. Your solution must ensure the smallest possible convergence time between the seven WINS servers.

What should you do?

A.   Configure your WINS server and the WINS servers in the subsidiary's main office as push/pull partners with each other.

Configure the WINS servers in the subsidiary's branch offices as pull partners with one WINS server in the subsidiary's main office.
B.   Configure your WINS server and the WINS servers in the subsidiary's main office as push/pull partners with each other.
Configure the WINS servers in the subsidiary's branch offices as push/pull partners with one WINS server in the subsidiary's main office.
C.   Configure all WINS servers to use the automatic partner configuration.
D.   Configure all WINS servers as push/pull partners with each other.

Answer: B
Explanation: For fastest convergence time we should configure PUSH/PULL partners. First we configure our WINS server as PUSH/PULL partner with the WINS servers and the partner's main office. Then we configure each branch office WINS server as a PUSH/PULL partner with one of the WINS servers at the partner's main office.

Incorrect Answers:
A: The suggested solution configures the branch office WINS server as a PULL partner to one of the WINS server in the partner's main office. But a PUSH/PULL configuration has faster convergence time than a PULL configuration.
C: Automatic partner configuration will not work. The network topology is too complex.
D: This would work but it would decrease performance due to unnecessary network traffic.

QUESTION NO: 226
You are the network administrator for Tailspin Toys. The network includes three UNIX-based Web servers named WWW1, WWW2, and WWW3. These servers host all Web pages for www.tailspintoys.com. For load balancing purposes, each server contains exactly the same content. The relevant portion of your network configuration is shown in the exhibit.
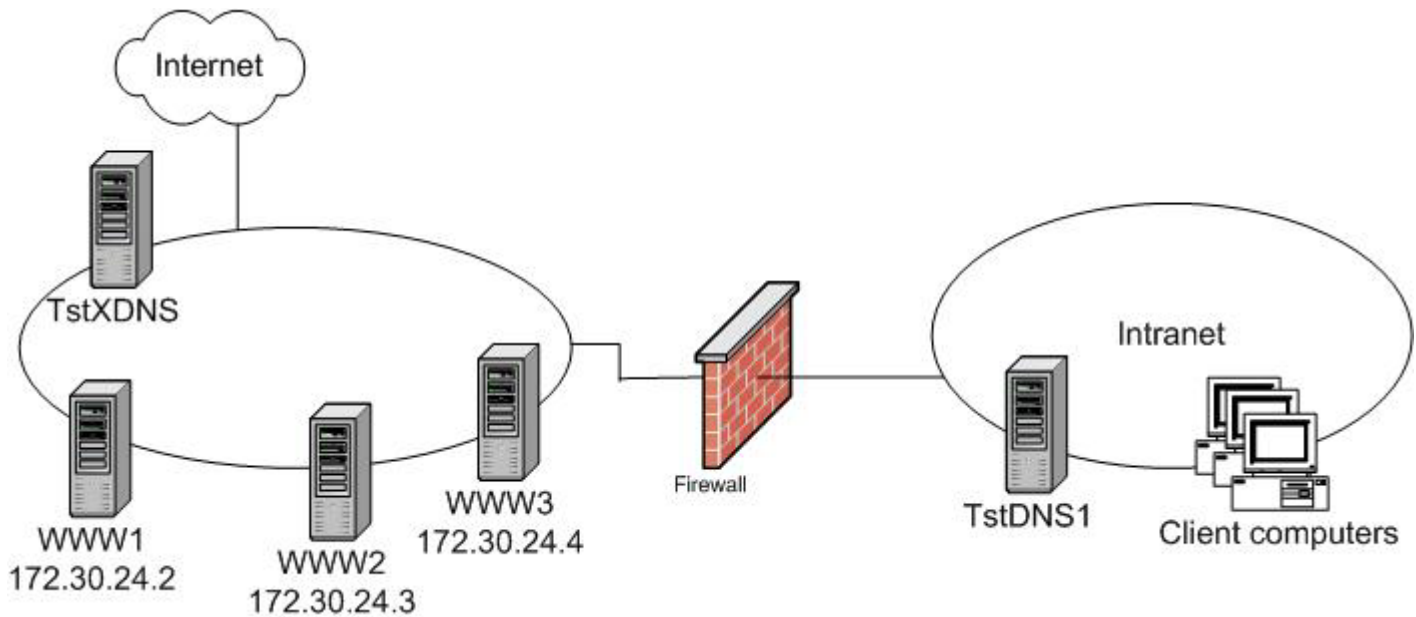
Client computers on your network are configured to use TstDNS1 for DNS name resolution. Internet users use TstXDNS to resolve names in the tailspintoys.com domain. TstDNS1 is not currently configured to use a forwarder.

Internal users report that access to www.tailspintoys.com is sometimes very slow. The DNS zone file on TstDNS1 currently contains an A (host) record for www.tailspintoys.com that points to 172.30.12.2.

You need to configure TstDNS1 to improve internal access to www.tailspintoys.com. What should you do?

To answer, click the Select and Place button, and then drag the correct DNS record types, host names, and DNS server options to the appropriate location. You might need to use some record types, host names, and server options more than once.

Record type	IP address	Host name
A	172.30.24.2	WWW
	172.30.24.3	
	172.30.24.4	

Record types	Host names
A	WWW1
CNAME	WWW2
SRV	WWW3
PTR	WWW

DNS server option

DNS server options

Enable round robin

Enable recursive queries

Enable dynamic updates

Answer:

Record type	IP address	Host name
A	172.30.24.2	WWW
A	172.30.24.3	WWW
A	172.30.24.4	WWW

Record types	Host names
A	WWW1
CNAME	WWW2
SRV	WWW3
PTR	WWW

DNS server option

Enable round robin

DNS server options

Enable recursive queries

Enable dynamic updates

Explanation: We enable load balancing by configuring the DNS server to enable round robin. Then we create three A (Host) records for each of the web servers using the same host name. When the DNS server resolves the host name WWW it will rotate through the three IP addresses 172.30.24.2, 172.30.24.3, and 172.30.24.4. This ensures proper load balancing.

Incorrect answers:
The DNS server option recursive queries is a configuration that enables forwarding on the DNS server. It doesn't apply in this scenario.
The DNS server option dynamic updates is a configuration that enables DHCP clients and DHCP servers to register the clients in DNS. This setting will not influence the load balancing of the Web servers.

We should not use CNAME (Alias) records, SRV records or PTR records. The Web servers are accessed through A (Host) records.

Round robin load balancing requires that all servers that are to be load balanced have the same host name in the DNS zone. Only the IP address differs.

QUESTION NO: 227
You are the administrator of TestKing's network, which includes one segment named Segment A. Your company employs 300 mobile salespeople who connect their portable computers to this segment.

Segment A includes a DHCP server that is configured with a single scope. The scope has the characteristics shown in the following table.

IP address range	Lease duration	Reserved IP address
172.20.100.05 to 172.20.100.254	Default setting	10

Half of the salespeople work on-site from 8:00 A.M. to 5:30 P.M. on Mondays, Wednesdays, and Fridays. These users work remotely on other business days. The other half of the salespeople work on-site from 8:00 A.M. to 5:30 P.M. Tuesdays and Thursdays. These users work remotely on other business days.

The salespeople who work on-site on Tuesdays and Thursdays report that they cannot connect to network resources.

You need to ensure that all salespeople can connect to network resources when they work on-site. You also want to minimize network traffic caused by DHCP services. What should you do?

A. Change the lease duration of the scope to 14 hours.
B. Change the lease duration of the scope to 9 hours.
C. Add IP address reservations for the computers used by the salespeople who work on-site Tuesdays and Thursdays.
D. Add IP address reservations for the computers used by the salespeople who work on-site Mondays, Wednesdays and Fridays.

Answer: A
Explanation: In Windows 2000, the default DHCP lease duration is 8 days. We have 300 mobile users but only 249 IP addresses in the IP address range. We must decrease the DHCP lease duration so that an IP address used by one remote computer can be used by another remote computer the next day. By changing the lease duration to 14 hours this will be accomplished.

Incorrect Answers:
B: A lease duration of 9 hours would enable the reuse of IP addresses from one day to another. However, it would not minimize network traffic since a computer that receives a lease at 8 A.M. would attempt to renew the lease after 4.5 hours (50% of the lease time), then again after 6.75 hours (75% of the lease time) and so on until the lease is successfully renewed. This is unnecessary.
C, D: Adding IP address reservations would not free IP addresses for the following day.

QUESTION NO: 228
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The network has a persistent connection to the Internet. The relevant portion of its configuration is shown in the exhibit.
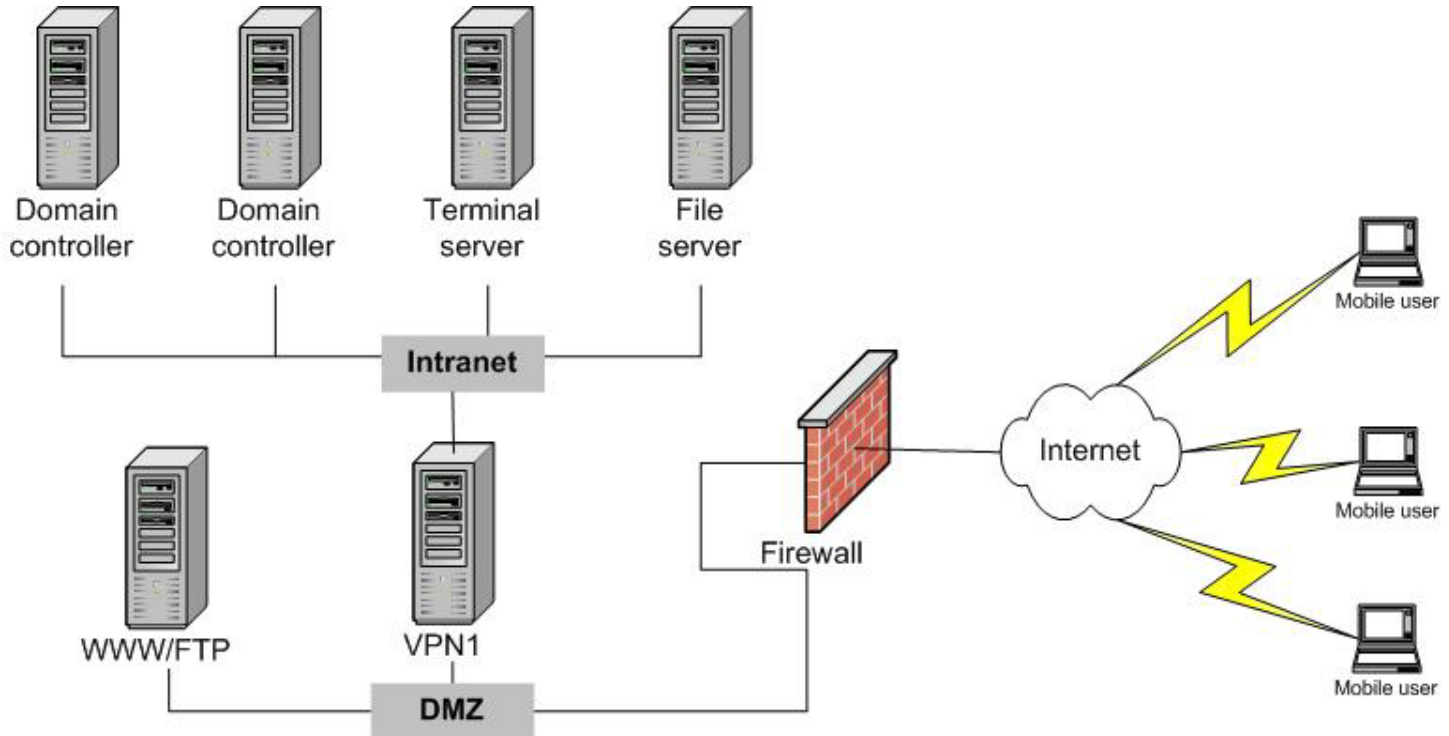
Your company employs mobile salespeople who use portable computers running Windows 98. To enable these users to access internal file and application resources, you place a virtual private network (VPN) server named VPN1 on the DMZ network inside your firewall. VPN1 is a Windows 2000 Server computer that runs Routing and Remote Access. You configure PPTP ports on VPN1. VPN users will initiate a Terminal Services client session to access internal resources.

Currently, the firewall allows inbound access only to TestKing's Web and FTP sites. Now you must enable the mobile salespeople to connect to VPN1.

What should you do?

A.   Create inbound packet filters on the firewall. Use PPTP as the destination protocol and port. Use the
        IP address of the firewall as the destination IP address.
        Create outbound packet filters on the firewall. Use PPTP as the source protocol port. Use the IP
        address of the firewall as the source IP address.
B.   Create inbound packet filters on the firewall. Use PPTP as the source protocol and port. Use the IP
        address of the firewall as the source IP address.
        Create outbound packet filters on the firewall. Use PPTP as the destination protocol port. Use the IP
        address of the firewall as the destination IP address.

C.   Create an inbound packet filter on the firewall. Use the Terminal server port as the destination port. Use the IP address of the Terminal server as the destination IP address.
Create an outbound packet filter on the firewall. Use the Terminal server port as the source port. Use the IP address of the Terminal server as the source IP address.

D.   Create an inbound packet filter on the firewall. Use the Terminal server port as the source port. Use the IP address of the Terminal server as the source IP address.
Create an outbound packet filter on the firewall. Use the Terminal server port as the destination port. Use the IP address of the Terminal server as the destination IP address.

Answer: C
Explanation: The mobile clients will try to initiate communication with the Terminal servers. Therefore the firewall must have an inbound packet filter where the Terminal server port is the destination port and the Terminal server IP address as the destination IP address.
The Terminal server must also be able to communicate with the mobile computers. The firewall must be configured with an outbound packet filter where the Terminal server port is the source port and the IP address of the Terminal server is the source IP address.

Incorrect Answers:
A: The destination port and IP address of the inbound packet filter must be set to the Terminal server, not to the firewall. The firewall could be the destination port and IP address if the VPN server was outside the firewall.
B: The inbound packet filter cannot have the firewall has source address.
D: The inbound packet must use the Terminal server port as destination port, not source port.

QUESTION NO: 229
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. Company employees need to access network resources when they are working remotely. Some remote users have desktop computers that run Windows 95, Windows 98, or Windows 2000 Professional. Other remote users have company-issued portable computers that run Windows 2000 Professional.

To provide secure access for all remote users, you enable Routing and Remote Access on a Windows 2000 Server computer that is connected to the Internet. You also create ports for 25 PPTP virtual private network (VPN) connections. You verify that all VPN client connections are configured correctly.

To ensure security, you create a Routing and Remote Access policy and configure authentication as shown in the exhibit.
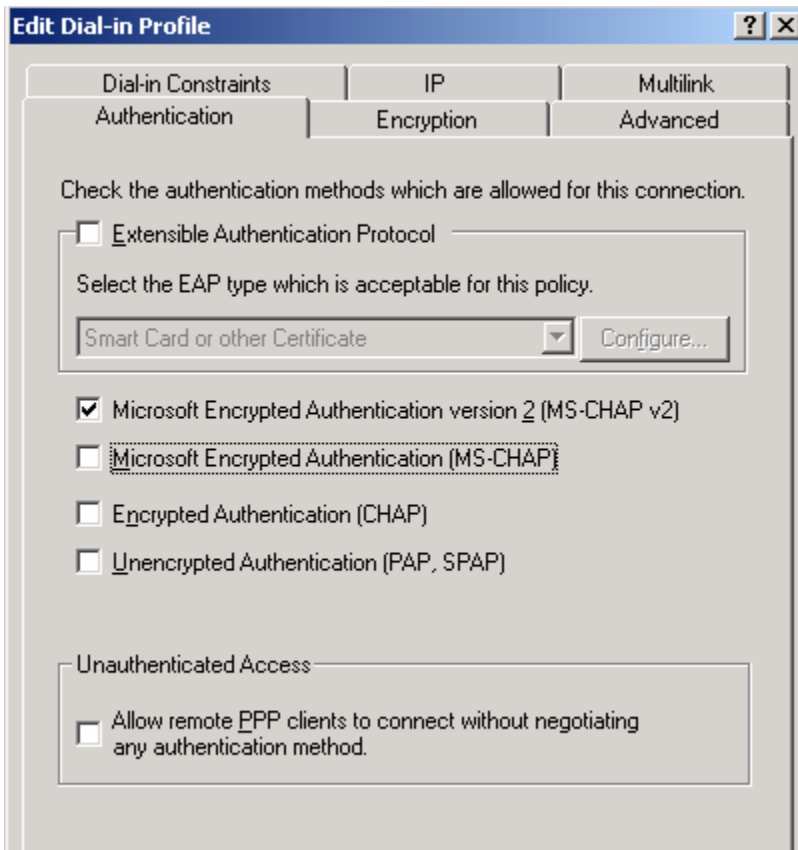
All remote users of Windows 2000 Professional can new connect to the VPN server successfully. No other remote users can establish a connection.

You need to enable all remote users to connect to the VPN server, regardless of client operating system. You also need to ensure the highest possible level of authentication security.

What should you do?

A.   Select the **Extensible Authentication Protocol** check box and select **MD-5 Challenge** in the list box.
B.   Select the **Microsoft Encrypted Authentication (MS-CHAP)** check box.
C.   Select the **Encrypted Authentication (CHAP)** check box.
D.   Select the **Unencrypted Authentication (PAP, SPAP)** check box.

Answer: B
Explanation: Windows 95 and Windows 98 don't support MS-CHAP V2 without additional windows update packages. This is the reason that only the Windows 2000 remote users can connect to the network. However, Windows 95 and Windows 98 do support the MS-CHAP authentication protocol.

Incorrect Answers:

A: EAP would require further configuration to function.
C: MS-CHAP is more secure than CHAP.
D: MS-CHAP is more secure than PAP and SPAP.

QUESTION NO: 230
You are the network administrator for Trey Research. Your network consists of a single Windows 2000 domain. All servers run Windows 2000 Server and all client computers run Windows 2000 Professional.

The network contains three domain controllers, which run the services shown in the following table.

Domain controller	Network services
DC1	DNS, global catalog
DC2	WINS
DC3	DHCP, Certificate Services

DC1 hosts an Active Directory integrated zone, which is configured to require secure dynamic updates. All servers have static IP addresses and all client computers are DHCP clients. All computers are configured to register their addresses with DNS.

Users report slow response times when they query the directory. Several users report that they cannot query the directory at all. When you view the event logs on DC1, you find the following event messages.

```
Event ID: 4011

The DNS server was unable to add or write and update of domain name _ldap
in zone treyresearch.com to the Active Directory. Check that the active
Directory is functioning properly and add or update this domain name using
the DNS console. The event data contains the error.

The DNS server was unable to add or write and update of domain name _gc in
zone treyresearch.com to the Active Directory. Check that the active
Directory is functioning properly and add or update this domain name using
the DNS console. The event data contains the error.

The DNS server was unable to add or write and update of domain name gc in
zone treyresearch.com to the Active Directory. Check that the active
Directory is functioning properly and add or update this domain name using
the DNS console. The event data contains the error.
```

You also discover the following error message, which was logged by the Netlogon service.

```
Event ID: 5781
Dynamic registration or deregistration of one or more DNS records failed
because no DNS servers are available.
```

Leading the way in IT testing and certification tools, www.testking.com

You verify that the DNS Server service is running on DC1. When you examine the DNS zone database, you discover that SRV (service) records for DC1 are not being registered. However, SRV records for DC2 and DC3 are being registered.

How should you correct this problem?

    A.   Install the DNS Server service and create an Active Directory integrated zone on DC2.
    B.   Configure the primary DNS server address of DC1 with its own IP address.
    C.   Reconfigure the treyresearch.com zone on DC1 so that it does not require secure dynamic updates.
    D.   Configure DC2 as a global catalog server and remove the global catalog from DC1.

Answer: D
Explanation: The cause of this problem is that the DNS server hosts an Active Directory integrated zone on a Domain controller which at the same time is running the Global catalog service. The best solution of this problem is to move the global catalog service from the DNS server DC1 to the WINS server DC2.

Reference: DNS Server Generates Event 4011 (Q252695)

Incorrect Answers:
A: It would, if possible at all, require a lot administrative effort to move the DNS service from DC1 to DC2.
B: This is a problem with the Global catalog service, not a DNS configuration problem.
C: This is a problem with the Global catalog service, not a DNS configuration problem.

QUESTION NO: 231
You are the network administrator for TestKing. Your network consists of a single Windows 2000 domain in native mode, and it includes a Routing and Remote Access server named RAS1. RAS1 is located in TestKing's New York office.

Company employees who travel to Singapore must dial in to RAS1 for network access. These employees use Windows 2000 Professional computers.

You need to ensure that these dial-up connections are as secure as possible. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

    A.   Configure RAS1 to require Microsoft Point-to-Point Encryption (MPPE) for all dial-up users.
    B.   Configure RAS1 to require L2TP connections for all dial-up users.
    C.   Configure RAS1 to require MS-CHAP v2 authentication.
    D.   Configure RAS1 to require EAP-CHAP authentication.
    E.   Install a server encryption certificate on RAS1.
    F.   Install an encryption certificate on all client computers.

Answer: A, C
Explanation: MS-CHAP V2 with MPPE would provide secure remote connections.

Incorrect Answers:
B: L2TP would require IPSec to provide security.
D: The EAP-CHAP protocol is not supported by Windows 2000.
E: To be able to use the server encryption certificate further configuration would be required.
F: To be able to use encryption certificates on the client computers further configuration would be required.

QUESTION NO: 232
You are the network administrator of the TestKing Insurance network, which consists of a single Windows 2000 domain named testking.com. The relevant portion of the network configuration is shown in the exhibit.
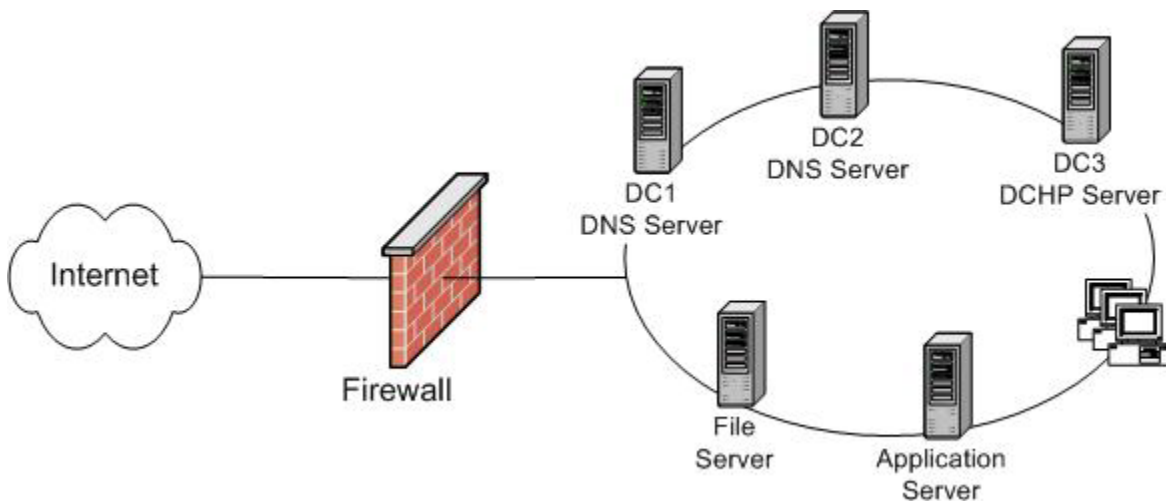
Two domain controllers named DC1 and DC2 run the DNS Server service and host an Active Directory integrated zone for testking.com. DC1 and DC2 are configured to allow dynamic updates to the zone database and to forward all unknown name resolution requests to a DNS server hosted by your Internet service provider (ISP).

All client computers are DHCP clients, and all servers have static IP addresses. All computers are configured to register their addresses with DNS.

When you monitor network traffic, you discover several DNS queries and error responses relating to a server named blackhole.isi.edu. On investigation, you discover that these queries are dynamic DNS registration requests from your network to an external DNS server.

You must prevent these registration requests from leaving your network. However, you must also ensure that your DNS servers continue to forward requests.

What should you do?

    A.   Create a root zone on your DNS servers.
    B.   Create a reverse lookup zone for 30.172.in-addr.arpa on your DNS servers.
    C.   Configure the zone to allow only secure dynamic updates.
    D.   Disable recursion on your DNS servers.

Answer: B
Explanation: Microsoft identifies this problem in KB Q259922. This behavior can occur when Windows 2000 tries to register the DNS PTR (reverse-lookup) record for a private network address. Two proposed solutions given are:
- Configure your local DNS server to have the reverse-lookup zone that the Windows 2000-based computers can use to register. This reverse lookup zone should be configured for your private IP address range. If you use the 10.0.0.0 network the reverse lookup zone should be 10.in-addr.arpa.
- Add a registry entry DisableReverseAddressRegistrations with value 1. This would disable ReverseAddressRegistrations.

The private IP address range on the network seems to in the 172.30.0.0/16 range. This is a private IP address range. The reverse lookup zone for this network is 30.172. in-addr.arpa. We should create a reverse lookup zone for this network to resolve the problem.

Reference:
DNS Request for blackhole.isi.edu (Q259922)
Valid IP Addressing for a Private Network (Q142863)

Incorrect Answers:
A: Creating a new root zone would not help.
C: This is not a DNS security problem.
D: Disabling recursions would not resolve the problem. It is a reverse-registration problem, not a host to IP resolution problem.

QUESTION NO: 233
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The relevant portion of its configuration is shown in the exhibit.
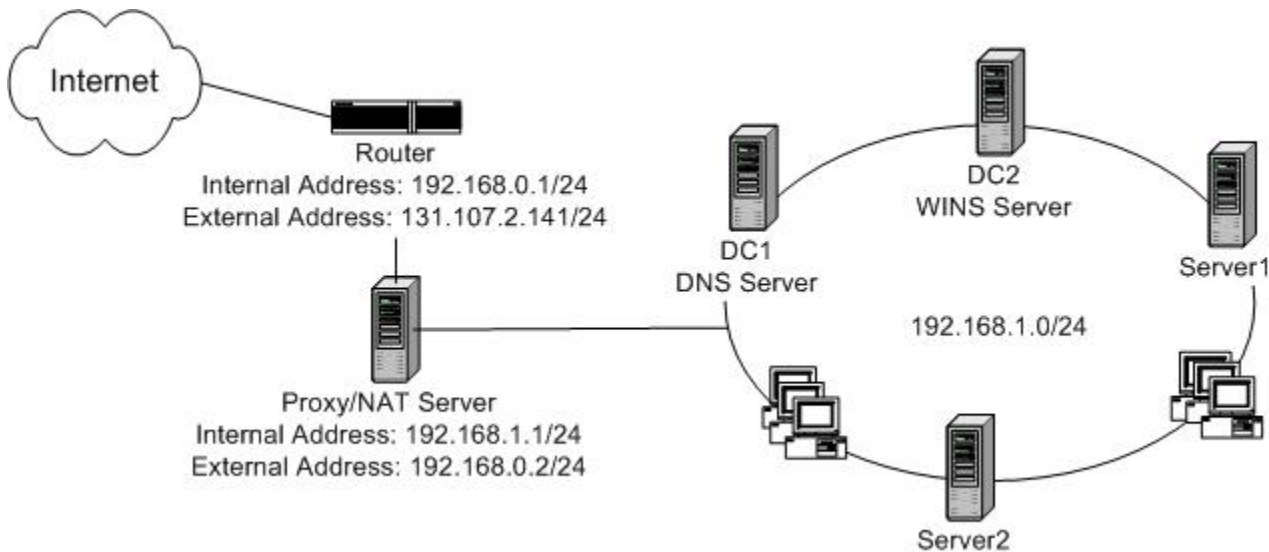
The network contains 200 client computers running Windows 2000 Professional. All client computers and all servers have static IP addresses.

You install the DHCP Server service on DC1. You configure a scope to provide IP addresses and appropriate configuration options to all client computers. Servers retain their static IP configurations.

Users now report that they receive error messages stating "Destination host unreachable" when they try to access the Internet. They have no problems connecting to internal network resources. Servers have no problems with Internet connectivity.

You inspect the routing table on a representative client computer. You find the information shown in the following table.

Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.175	192.168.1.175	1
192.168.1.175	255.255.255.255	127.0.0.1	127.0.0.1	1
255.255.255.255	255.255.255.255	192.168.1.175	192.168.1.175	1
224.0.0.0	224.0.0.0	192.168.1.175	192.168.1.175	1
255.255.255.255	255.255.255.255	192.168.1.175	192.168.1.175	1

You need to enable all users to access the Internet. What should you do?

A. Add a DHCP scope Static Route option with values of 131.107.2.0 for the IP address and 192.168.1.1 for the gateway.
B. Add a DHCP scope Static Route option with values of 131.107.2.0 for the IP address and 192.168.0.1 for the gateway.
C. Add a DHCP scope Router option with a value of 192.168.1.1.
D. Add a DHCP scope Router option with a value of 192.168.0.1.

Leading the way in IT testing and certification tools, www.testking.com

Answer: C
Explanation: The table indicates that the default gateway setting on the client is 192.168.1.175 instead of the IP address of the internal interface on the Proxy/NAT Server 192.168.1.1. We should configure the Router option in the DHCP scope to this address.

Incorrect Answers:
A, B: The Servers can reach Internet so there would not be any need to add any Static routes.
D: The Router option, also called the Default gateway, should be configured with the IP address of the internal interface on the Proxy/NAT server. The IP address 192.168.0.1 is the IP address of the internal interface on the router, and the router can only reached through the NAT server.

QUESTION NO: 234
You are the network administrator for TestKing Insurance. The relevant partition of your network configuration is shown in the exhibit.
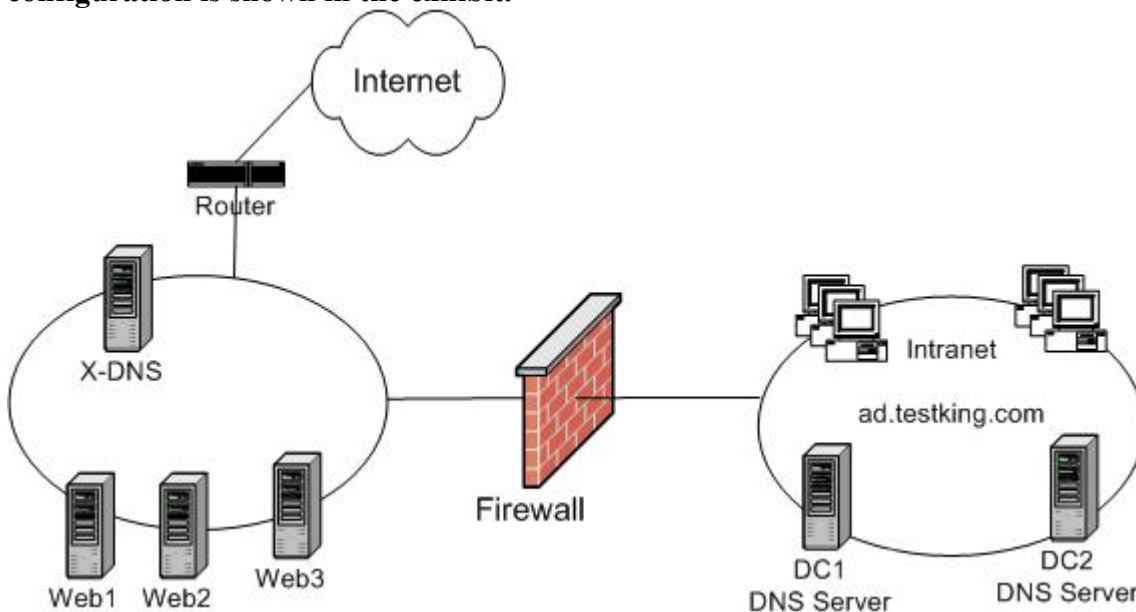
The network includes three Web servers named Web1, Web2, and Web3. All three run Windows 2000 Server and host the Web pages for TestKing's Web site, which is named www.testking.com. For load balancing purposes, each Web server contains exactly the same content.

The company intranet consists of a single Windows 2000 domain. Two domain controllers, DC1 and DC2, host an Active Directory integrated zone for the domain. Client computers on the intranet are configured to use DC1 and DC2 for DNS name resolution. External customers use a UNIX-based DNS server, X-DNS, to resolve names in the testking.com domain.

**Company policy states that no external IP addresses can be hosted on internal DNS servers, and no
internal IP addresses can be hosted on external DNS servers.**

**Internal users report that they cannot access the new Web site from the intranet. External customers
report that access to the Web site is extremely slow.**

**You need to reconfigure DC1 and DC2 to allow internal access to the company Web site and to improve
access times for external customers.**
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A.   Add A (host) records named Web1, Web2, and Web3 to the zone hosted on X-DNS.
B.   Add A (host) records named Web1, Web2, and Web3 to the zone hosted on DC1 and DC2.
C.   Add A (host) records named WWW for the three Web servers to the zone hosted on X-DNS.
D.   Add A (host) records named WWW for the three Web servers to the zone hosted on DC1 and DC2.
E.   Enable round robin on X-DNS and enable forwarding on DC1 and DC2.
F.   Enable round robin on DC1 and DC2 and enable forwarding on X-DNS.

Answer: C, E
Explanation:
C: We add three A (host) records with the same host name with the IP addresses of the three web servers.
E: We enable load balancing by configuring the DNS server to enable round robin. When the DNS server
          resolves the host name WWW it will rotate through the three Web1, Web2, and Web3. This ensures
          proper load balancing.
          Finally we enable forwarding on DC1 and DC2 so that the internal DNS server will forward external
          name resolution requests to the X-DNS server.

Incorrect Answers:
A: We must create three records with the same host name, not three different host names.
B: We are not allowed to add external host names to the internal DNS servers. Furthermore we must create
          three records with the same host name, not three different host names.
D: We are not allowed to add external host names to the internal DNS servers.
F: We must enable round robin on the external DNS server. We must enable forwarding on the internal
          DNS servers. Here we do the opposite.

QUESTION NO: 235
**You are the DHCP administrator for a very large company, namely TestKing. To enable employees to
participate in meetings and training sessions from their desks, TestKing plans to use streaming video
over the company network. You will be using a video conferencing technology that allows all participants
in the conference to access the same transmission. You anticipate that a maximum of 10,000 unique
groups will require support in the near future.**

You need to configure your DHCP servers to support automatic group address assignment for the video conferencing. What should you do?

A.   Create a multicast scope for the 239.192.0.0/14 network.
B.   Create a multicast scope for the 223.224.192.0/14 network.
C.   Create a multicast scope for the 239.192.0.0/20 network.
D.   Create a multicast scope for the 223.224.192.0/20 network.

Answer: A
Explanation:
Multicast is a scheme for using IP addresses 224.0.0.0 through 239.255.255.255 to send the same data to several machines simultaneously. Every IP datagram whose destination address starts with "1110" is an IP Multicast datagram.

239.192.0.0/14 is defined to be the IPv4 Organization Local Scope, and is the space from which an organization should allocate sub-ranges when defining scopes for private use.

Reference:
RFC2365
Multicast over TCP/IP HOWTO
What Is IP Multicast? (Q165011)
Differences Between Multicast and Unicast (Q291786)

Incorrect Answers:
B: The Multicast addresses range is from 224.0.0.0 to 239.255.255.255. We cannot use the 223.224.192.0/14 network for multicasting.
C: The 239.192.0.0/20 network would not allow 10,000 unique groups.
D: The Multicast addresses range is from 224.0.0.0 to 239.255.255.255. We cannot use the 223.224.192.0/14 network for multicasting.

QUESTION NO: 236
You are the network administrator for TestKing which operates a main office in San Diego and a newly acquired branch office in Los Angeles. The San Diego office maintains a firewall that allows only outbound web traffic and Virtual Private Network (VPN) traffic to the Internet. In front of this firewall a router is connected to a local Internet Service Provider (ISP). The San Diego office also includes an L2TP server named VPN1 with a persistent connection to the Internet. VPN1 bypasses the firewall.

Another server in San Diego, DB1, services a sales database used by employees in both offices. Users in Los Angeles need access to DB1 24 hours a day, 7 days a week. To supply this access, you install a new Windows 2000 Server computer named DPCIT1 in Los Angeles. Now you need to configure DPCIT1 so that users in Los Angeles can access DB1. What should you do?

A. Configure DPCIT1 as a dial-up client to connect to DB1. Enable IP Forwarding and configure static routes to San Diego.
B. Configure DPCIT1 as a demand-dial router to connect to the router in front of the firewall in San Diego.
C. Configure DPCIT1 for RIP routing and a persistent connection to VPN1
D. Contact your Internet service provider in Los Angeles and configure DPCIT1 as an OSPF router on the Internet

Answer: C
Explanation: A persistent connection to from DPCIT1 to VPN1 would provide Los Angeles users with access to the San Diego Server DB1.

Note: The following illustration is not included in the scenario. It is only included in the explanation out of illustrative purposes.
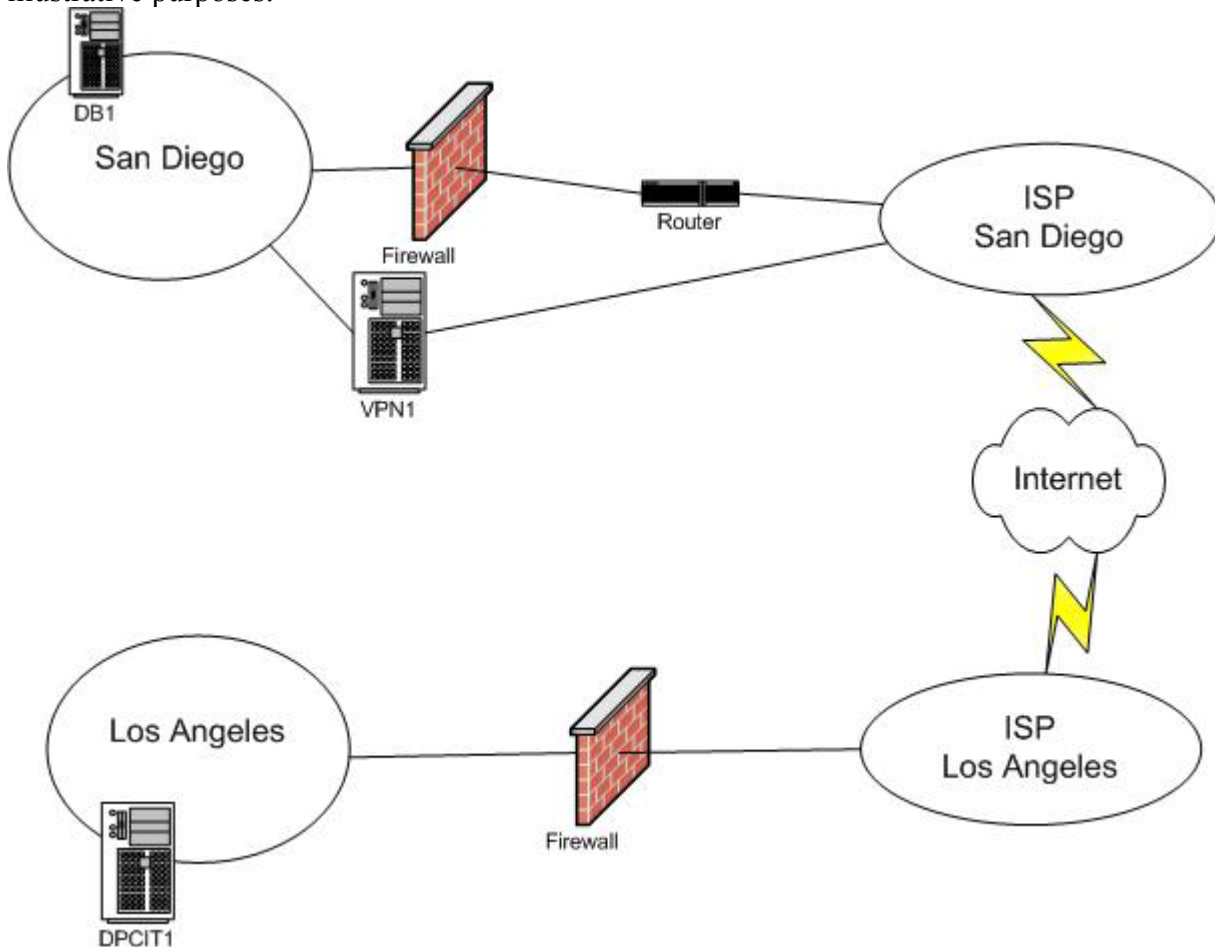
Incorrect Answers:
A: DPCIT1 in Los Angeles cannot be a dial-up client of DB1 in San Diego. DB1 is behind the Firewall and VPN.

B: The San Diego firewall only allows VPN inbound traffic. It would not allow a connection from DPCIT1 to the San Diego Router.

D: DPCIT1 should not be configured as Internet Router.

QUESTION NO: 237
You are the administrator of TestKing's network. You need to implement a remote access solution that is highly available and highly secure. Your company consists of a single location and has a T3 connection to the Internet.

Your company has 1,000 salespeople who need reliable connectivity to the company network from any remote location. All servers are running Windows 2000 Advanced Server, and all client computers are running Windows 2000 Professional.

You want to accomplish the following goals:

- No single point of failure, aside from total loss of the T3, will result in total loss of remote access connectivity.
- No authentication traffic will be carried as clear text.
- No data traffic will be carried as clear text.
- Support for at least 200 simultaneous remote users accessing the network will be available at all times.

You take the following actions:

- Install a virtual private network (VPN) server at the main office.
- Configure the VPN server to support 250 PPTP connections.
- Configure the client computers to use Challenge-Handshake Authentication (CHAP) as the authentication protocol.

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

A. No single point of failure, aside from total loss of the T3, results in total loss of remote access connectivity.
B. No authentication traffic is carried as clear text
C. No data traffic is carried as clear text
D. Support for at least 200 simultaneous remote users accessing the network is available at all times

Answer: B, D.
Explanation:
B: The CHAP authentication protocol uses reversible password encryption. No authentication traffic will be sent as clear text.

D: One VPN server with 250 PPTP ports will support at least 200 simultaneous remote users at all times, unless the VPN server itself malfunctions.

Incorrect Answers:
A: The single VPN server is the single point of failure. If the VPN server malfunctions there would be no remote access.
C: PPP encryption requires either EAP-TLS, MS-CHAP or MS-CHAP v2 in combination with Point-to-Point Encryption (MPPE) to encrypt data. PPP does not provide data encryption.

QUESTION NO: 238
TestKing's network consists of two Windows 2000 domains named corp1.local and research1.local. Both domains are forest roots. You are administrator in corp1.local.

Your network includes a DHCP server named WinDHCP1, which is a member of corp1.local. WinDHCP1 experiences a hardware failure and cannot be restarted.

You decide to install the DHCP Server service on a Windows 2000 Server computer named Rfiles1. You obtain the password for the local Administrator account on Rfiles1 and install the DHCP Server service. After the installation is complete, you try to start the service. However, it immediately stops.

When you examine the DHCP Server log on Rfiles1, you discover the following entries.

```
ID Date, Time, Description, IP Address, Host Name, MAC Address
00, 06/27/00, 11:23:09, Started,,,
60, 06/27/00, 11:23:32, No DC is DS Enabled,,Research1,
63, 06/27/00, 11:23:50, Restarting rogue detection,,,
01, 06/27/00, 11:58:11, Stopped,,,
```

You need to correct the problem and start the DHCP Server service on Rfiles1. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

   A.   Use the Active Directory Sites and Services console in corp1.local to authorize Rfiles1 as a DHCP Server.
   B.   Use the Active Directory Sites and Services console in research1.local to authorize Rfiles1 as a DHCP Server.
   C.   Change the domain membership of Rfiles1 so that it is a member of a workgroup named research1.
   D.   Change the domain membership of Rfiles1 so that it is a member of corp1.local.
   E.   Configure the DHCP Server service to log on to the network by using a corp1.local user account that is a member of the Domain Admins group.

Leading the way in IT testing and certification tools, www.testking.com

Answer: A, D
Explanation:
A: The new DHCP server must be authorized in the Active Directory. The new DHCP server should be authorized in the corp1.local domain, the same domain as the failed DHCP Server.
D: By examining the DHCP server log we see that the DHCP server searches for a Domain Controller in the Research domain. The DHCP server computer must belong to the corp1.local domain however. We must change the domain membership of Rfiles1 computer to corp1.local.

Incorrect Answers:
B: The DHCP server should be authorized in the corp1.local domain, not in the research1.local domain.
C: The exhibit shows that the Rfiles1 computer searches for a Domain Controller in the research1.local domain. Rfiles1 already belongs to the research1.local domain, but needs to a member of the corp1.local domain.
E: There is no requirement for the DHCP server to run in the context of a Domain Admins group. On the contrary this could be a security risk.

QUESTION NO: 239
You are the network administrator for TestKing Inc., and for Contoso Ltd, which is a subsidiary of TestKing Inc. Your network consists of three domains in four Active Directory Sites. The relevant portion of your network configuration is shown in the exhibit.
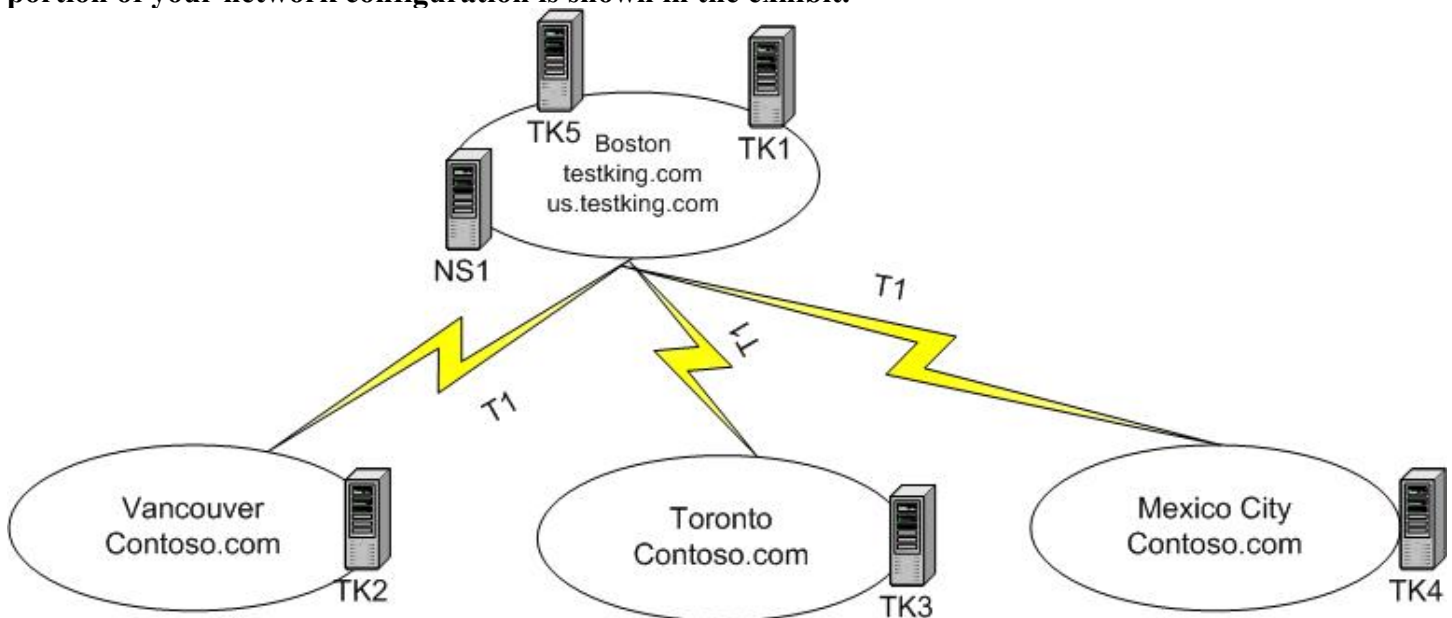
Your Active Directory structure is shown in the Active Directory Structure exhibit.
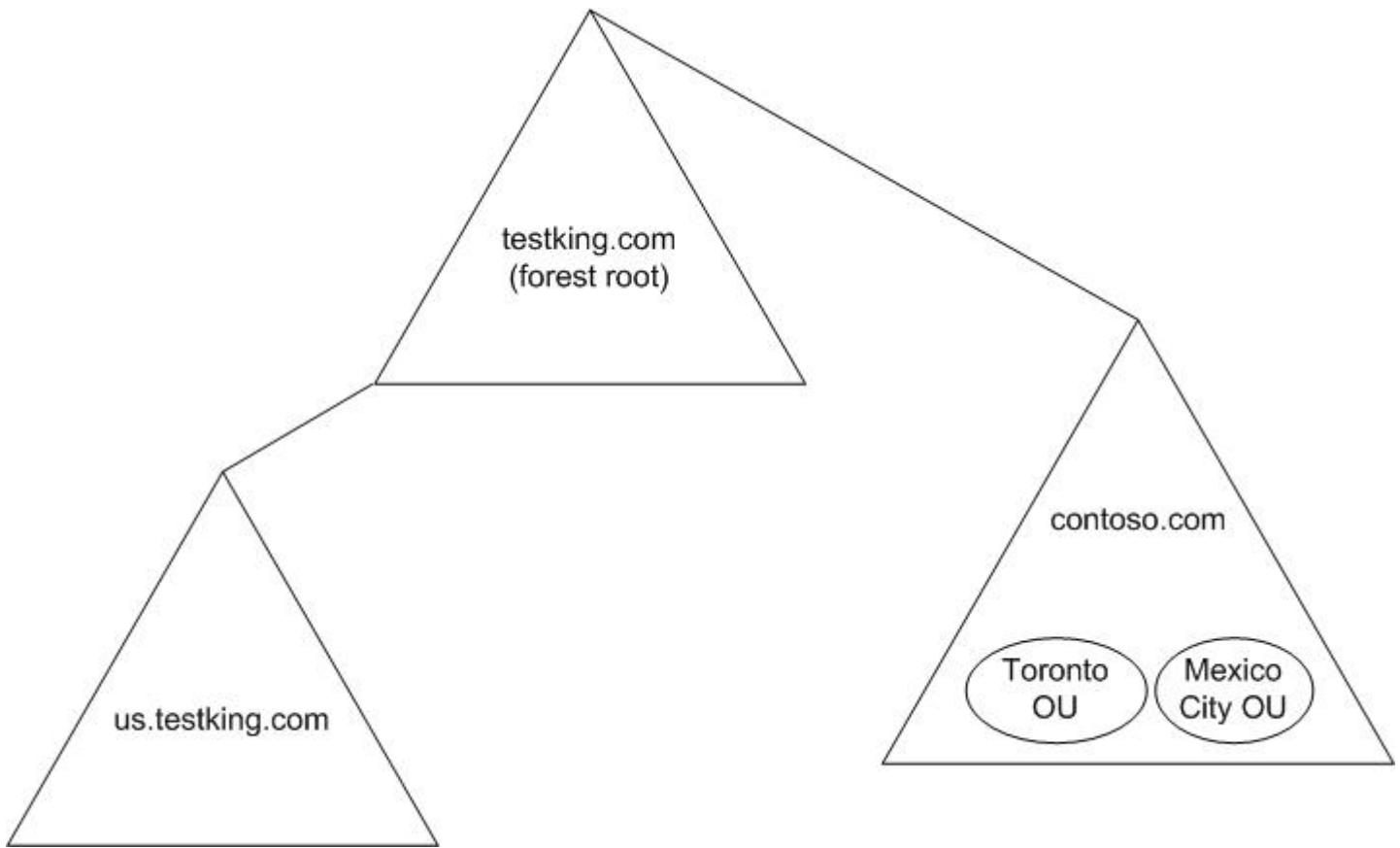
The Vancouver, Toronto, and Mexico City Offices are connected to the main office in Boston by means of T1 Lines. Each of these offices contains one DNS server running UNIX and BIND version 4.9.3. Toronto and Mexico City are organizational units (OUs) within the contoso.com domain.

You install a DNS server named ns1.testking.com at the main office. It hosts the zones shown in the following table.

Zone	Zone type	Allow dynamic updates?
testking.com	Active Directory	Yes
contoso.com	Standard primary	Yes
us.testking.com	Standard primary	Yes

Users in Mexico City, Toronto, and Vancouver report slow response times when they try to log on to their own domains. You discover that DNS registration and name resolution queries are generating heavy traffic across the WAN links.

You need to improve network response times for users and reduce traffic over the WAN links. What should you do?

    A.   Move the zone files for each primary zone to the appropriate local server.
            Configure the DNS servers in Vancouver, Toronto, and Mexico City to forward unresolved requests to ns1.testking.com.
            Configure the client computers in each site to use the address of their local DNS server.
    B.   Upgrade all DNS servers for contoso.com to Windows 2000 Server with Active Directory integrated zones.
            Move the contoso.com zone to Vancouver and reconfigure ns1.testking.com as a secondary server for contoso.com.
            Configure the client computers in each site to use the address of their local DNS server.
    C.   Upgrade the DNS servers in Vancouver, Toronto, and Mexico City to Windows 2000 Server.
            Convert all primary zones on ns1.testking.com to Active Directory integrated zones.
            Configure the contoso.com servers to forward unresolved requests to ns1.testking.com.
            Configure the client computers in each site to use the address of their local DNS server.
    D.   Move the contoso.com zone files to the DNS server in Vancouver.
            Convert the contoso.com primary zone on ns1.testking.com to a secondary zone that uses the contoso.com zone as the master zone.
            Configure the client computers in each site to use the address of their local DNS server.

Answer: B
Explanation: The name resolution in the contoso.com is resolved at the central office Boston. This increases the name resolution traffic between the contoso.com offices (Vancouver, Toronto, and Mexico City Offices) and the main office. It would be better to use local DNS servers at these three locations for the name resolution in the contoso.com domain. To accomplish this we need Active Directory integrated zones.
This can be accomplished by:

1. Upgrade the UNIX BIND DNS servers to Windows 2000 DNS servers at Vancouver, Toronto, and Mexico City.
2. Use Active Directory integrated zones at Vancouver, Toronto, and Mexico City.
3. Move the contoso.com zone to one of the contoso.com offices, for example Vancouver.
4. Reconfigure ns1.testking.com as a secondary server for the contoso.com zone.
5. Configure the contoso.com DNS servers in Vancouver, Toronto, and Mexico City to forward unresolved queries to ns1.testking.com.
   This would provide name resolution of computers in the testking.com and the us.testking.com domains.
6. Configure the client computers in Vancouver, Toronto, and Mexico City to use the local DNS server for name resolution.

Incorrect Answers:
A: There cannot be several primary zones for the contoso.com domain. Only one primary zone can exist.
C: We must configure the DNS servers in Vancouver, Toronto, and Mexico City to resolve names in the contoso.com domain.

We cannot create an Active Directory Integrated zone for the contoso.com domain at ns1.testking.com since this computer is not a member in the contoso.com domain.

D: We should configure the DNS servers at Toronto and Mexico City to resolve names in the contoso.com domain as well, not only Vancouver. We need an Active Directory integrated zone to accomplish this.

QUESTION NO: 240
You are the administrator of TestKing's network. All computers on the network run Windows 2000. Two servers named DB1 and DB2 run back-end medical information databases that require high levels of security. DB1 is located at your main office in London. DB2 is located at a branch office in San Francisco. These two offices are linked by a persistent high-speed connection, which enables the two servers to communicate with each other.

Client computers directly access the two servers to query data. Client computers also access resources on the Internet.

According to company policy, communications between DB1 and DB2 must be secure and encrypted. Communications between the two servers and the client computers must also be secure and encrypted. You need to develop a solution that does not disrupt any client computer communications and that minimizes processor usage on client computers.

What should you do?

    A.   Configure DB1 and DB2 with the Server IPSec policy.
           Configure the client computers with the Client IPSec policy.
    B.   Configure DB1 and DB2 with the Client IPSec policy.
           Configure the client computers with the Client IPSec policy.
    C.   Configure DB1 and DB2 with the Secure Server IPSec policy.
           Configure the client computers with the Client IPSec policy.
    D.   Configure DB1 and DB2 with the Secure Server IPSec policy.
           Configure the client computers with the Server IPSec policy.

Answer: C
Explanation: All communications to and from DB1 and DB2 must be secure and encrypted. We must use the Secure Server (Require Security) security template on DB1 and DB2.
The client computers will only need to use the Client (Respond only) security template. If a client computer tries to access DB1 (or DB2), DB1 will request security and the client computer will comply.

Incorrect Answers:
A: All communications to and from DB1 and DB2 must be secure so we cannot use the Server (Request Security) security template on DB1 or DB2 since this would allow unsecure traffic.

Leading the way in IT testing and certification tools, www.testking.com

B: All communications to and from DB1 and DB2 must be secure so we cannot use the Client (Respond only) security template on DB1 or DB2 since this would allow unsecure traffic.

D: It would be unnecessary to use the Server (Request Security) security template on the clients. Client-to-client traffic would be encrypted. This is not required in the scenario. This would increase the processor usage on the clients. The clients only need to respond to security requests from DB1 and DB2. The clients only need to use the Client (Respond only) security template.

QUESTION NO: 241
You are the network administrator for TestKing's research department. TestKing's network consists of a single segment. The research department is assigned the 172.30.10.0/24 subnet.

The research subnet includes 100 client computers and one DHCP server. All client computers are DHCP clients. You configure the DHCP server with a single scope, which has the characteristics shown in the following table.

DHCP scope	IP address range	IP address reservations	IP address exclusions
172.30.10.0/24	172.30.10.6 to 172.30.10.160	172.30.10.2 and 172.30.10.3	172.30.10.11 to 172.30.10.15

You add 10 new servers to the research subnet. These servers have static IP addresses from the range 172.30.10.161 to 172.30.10.170. Your department now decides to add 75 new client computers to the subnet.

You need to reconfigure the DHCP server so that it will support these new client computers, without adversely affecting the existing DHCP clients.
What should you do?

A. Re-create the DHCP scope with a 25-bit subnet mask.
B. Extend the upper limit of the existing DHCP scope to include 172.30.10.254. Add an address exclusion of 172.30.10.161 to 172.30.10.170.
C. Add an additional scope with an address range of 172.30.11.10 to 172.30.11.100 to the DHCP server.
D. Add an additional scope with an address range of 172.31.10.1 to 172.31.10.200 to the DHCP server.

Answer: B
Explanation: We need support another 10 static IP addresses and 75 dynamic IP addresses. This can be accomplished by extending the upper limit of the existing scope from 172.30.10.160 to 173.30.10.254. After adding an address exclusion of 172.30.10.161 to 172.30.10.170 we have 83 (254-171) free IP addresses to lease. This is more than adequate.

Reference:
Increasing the Number of IP Addresses on a Subnet (Q255999)
HOW TO: Install and Configure a DHCP Server in a Workgroup in Windows 2000 (Q301187)

Incorrect Answers:

A: A 25-bit subnet mask would only leave 7 bits for the hosts. Only 126 hosts could be supported.

C: Two separate scopes on the same subnet is not a good solution. Computers with IP addresses from the second scope would not be able to communicate with existing computers (without adding a router to the network).

D: Two separate scopes on the same subnet is not a good solution. Computers with IP addresses from the second scope would not be able to communicate with existing computers (without adding a router to the network).

QUESTION NO: 242
You are the network administrator for TestKing. TestKing consists of four divisions: Marketing, Sales, Finance, and Corporate. You divide your network into four subnets, one for each division. These subnets are connected by three Windows 2000 Server computers, which are configured as network routers in a default configuration. The relevant portion of your network configuration is shown in the following diagram.
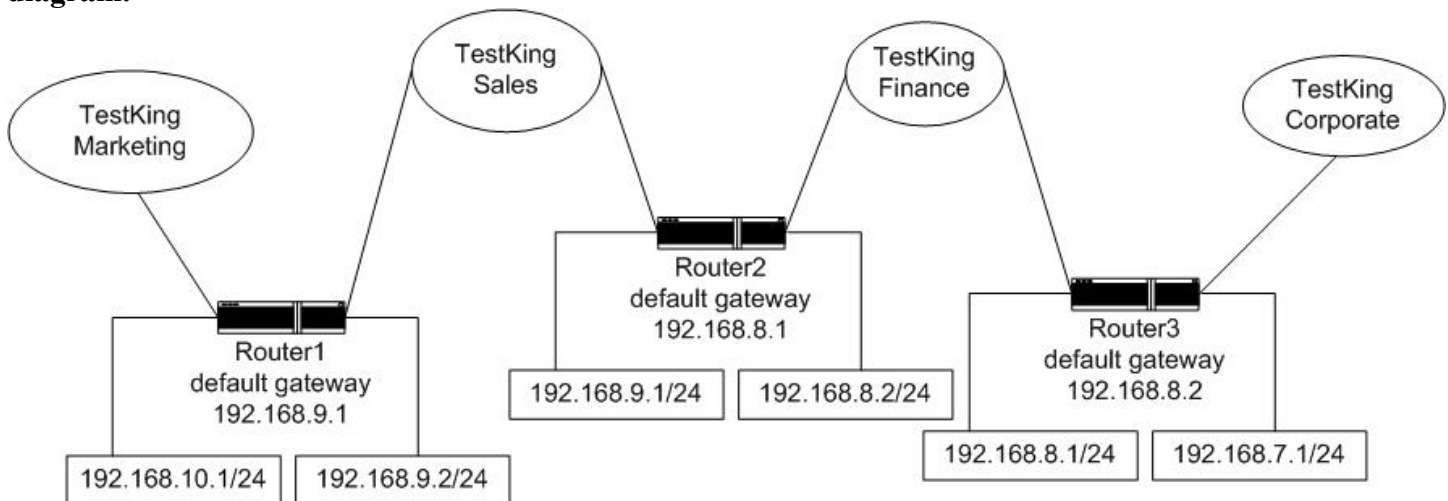
You need to enable all hosts on all subnets to communicate with each other. To accomplish this goal, you plan to add one or more static route entries to one or more of your routers.

Which static route entry or entries should you add, and where?

To answer, click the Select and Place button, and then drag the correct route entry or entries to the appropriate router or routers. Use the minimum number of necessary route entries and routers.

Select and Place

Possible route entries:
| 192.168.8.0/24 | 192.168.9.0/24 |
| 192.168.7.0/24 | 192.168.10.0/24 |

TestKing Sales

route entry

TestKing Finance

route entry

TestKing Marketing

route entry

TestKing Corporate

Router1
default gateway
192.168.9.1

Router2
default gateway
192.168.8.1

192.168.9.1/24   192.168.8.2/24

Router3
default gateway
192.168.8.2

192.168.10.1/24   192.168.9.2/24

192.168.8.1/24   192.168.7.1/24

Answer:

Possible route entries:

| 192.168.8.0/24 | 192.168.9.0/24 |

192.168.7.0/24
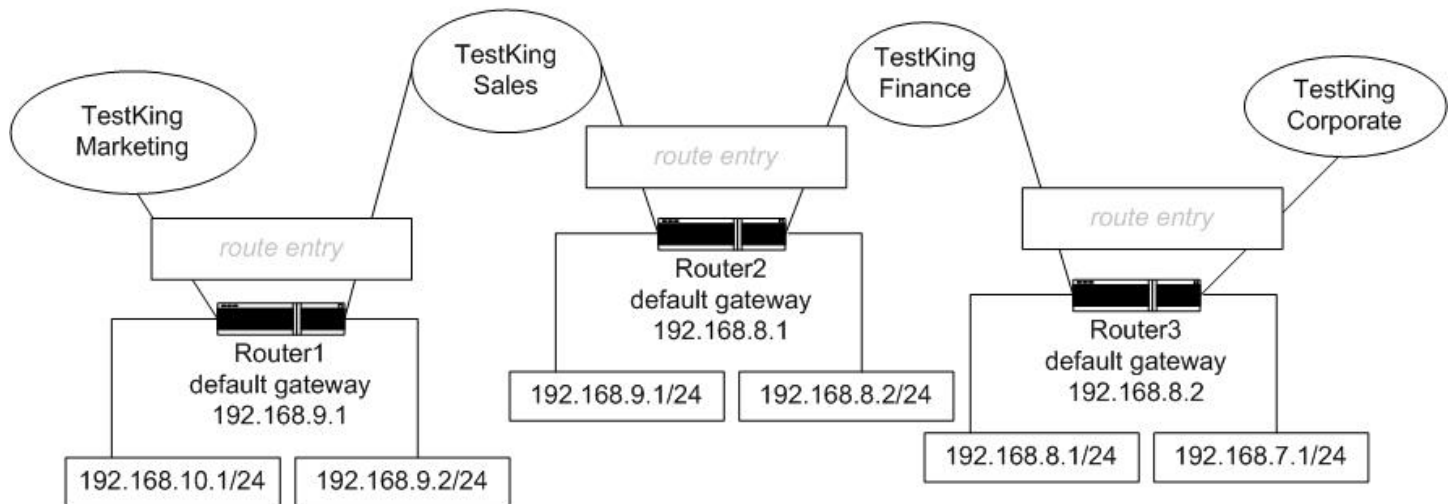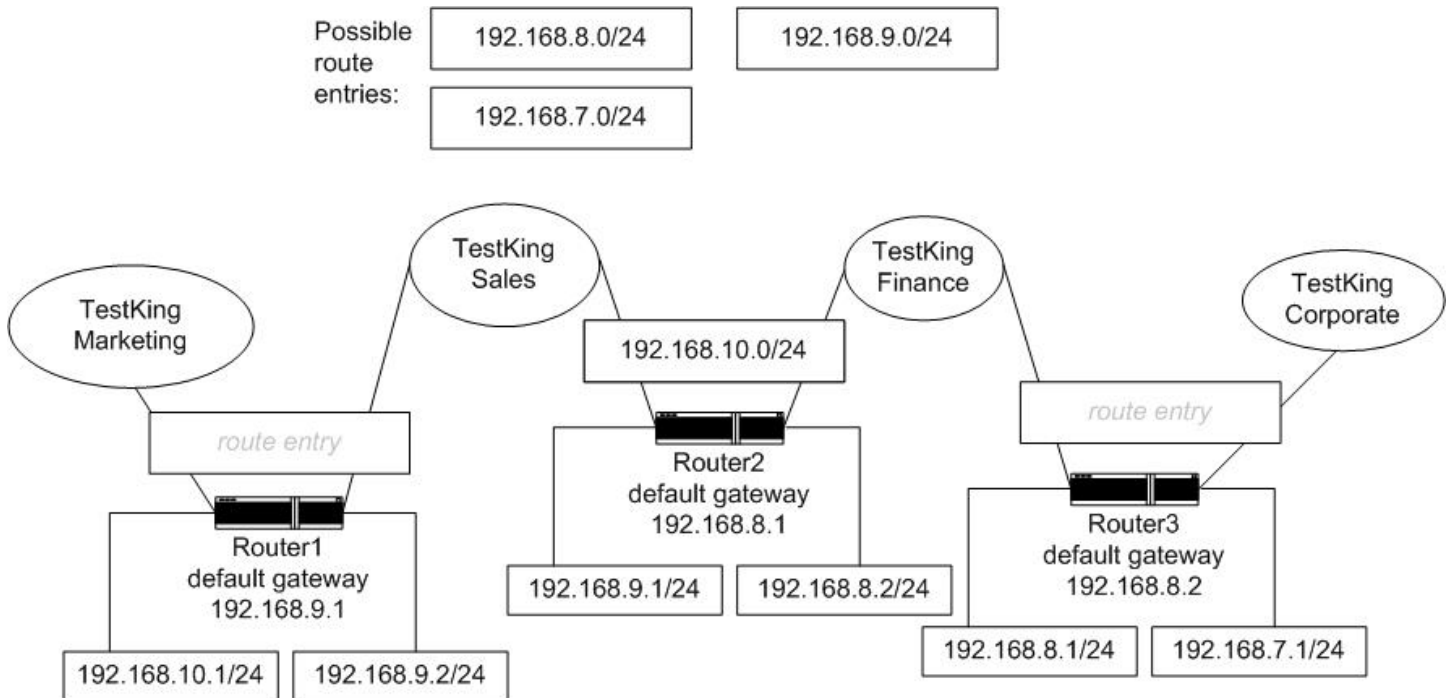
Explanation:
We must add a route for the 192.168.10.0/24 network to Router2.

If a client on the 192.168.10.0/24 subnet sends a packet to the 192.168.9.0/24 subnet, the packet will be sent to Router1 which knows how to get to the 192.168.9.0/24 subnet because Router1 is directly connected to the 192.168.9.0/24 subnet.
If a client on the 192.168.10.0/24 subnet sends a packet to the 192.168.8.0/24 subnet, the packet will be sent to Router1. Router1 doesn't know how to get to the 192.168.8.0/24 subnet so Router1 will forward the packet to it's default gateway which is Router2. Router2 knows how to get to the 192.168.8.0/24 subnet because Router2 is directly connected to the 192.168.8.0/24 subnet.

A similar thing will happen when a client on the Corporate subnet sends a packet to the Finance subnet. The problems will occur when a client on the Corporate subnet sends a packet to the Marketing subnet. If a client on the Corporate subnet (192.168.7.0/24) sends a packet to the Marketing subnet (192.168.10.0/24), the packet will be sent to Router3. Router3 doesn't know how do get to the Marketing subnet, so Router3 sends the packet to it's default gateway which is Router2. Router2 doesn't know how do get to the Marketing subnet, so Router2 sends the packet to it's default gateway which is Router3. The packet will be bounced between Router2 and Router3. Here we have a routing loop. To prevent this, we need to tell Router2 how to get to the Marketing subnet (192.168.10.0/24).

Leading the way in IT testing and certification tools, www.testking.com

QUESTION NO: 243
You are the administrator of TestKing's network. The relevant portion of its configuration is shown in the exhibit.
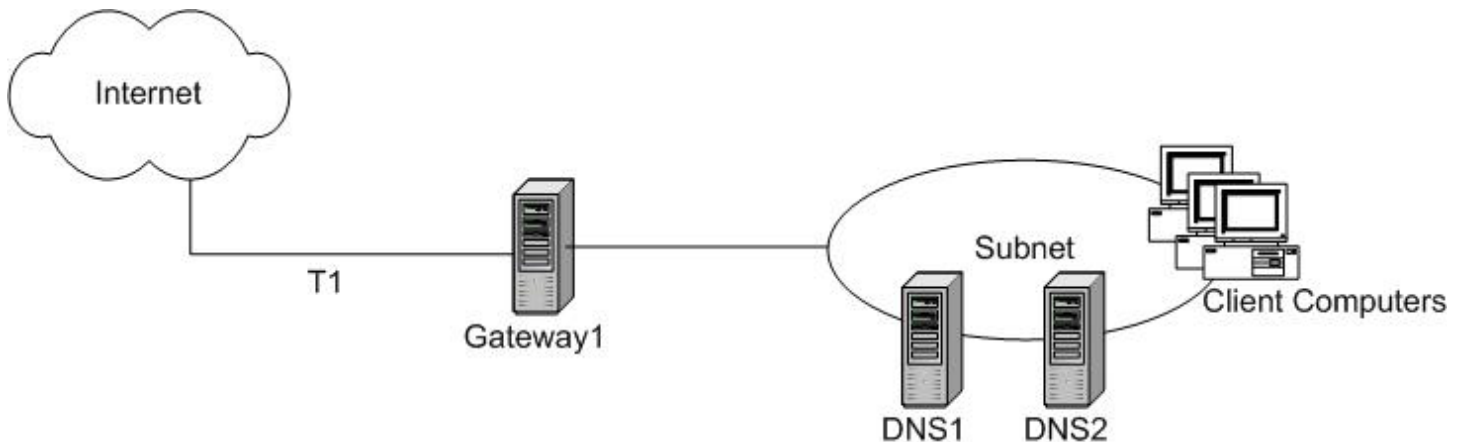
Gateway1 is a Windows 2000 Server computer that runs Routing and Remote Access. DNS1 and DNS2 are Windows 2000 Server computers that run the DNS Server service. All client computers run Windows 2000 Professional. Client computers are configured to use Gateway1 as their default gateway and DNS1 for name resolution. Internal users frequently browse Web sites.

Maria is an employee in the Accounting department. She reports that she always receives an error message when she tries to download a file from a particular Web site to her computer. The error message states "Connection timed out." Maria can successfully download files from other Web sites.

How should you correct this problem?

    A.   Configure Gateway1 to use DNS1 and DNS2 for name resolution.
    B.   Configure a TCP/IP packet filter on Gateway1 to pass FTP traffic.
    C.   Configure Maria's computer to use DNS2 as a secondary server for name resolution.
    D.   Run the **ipconfig /flushdns** command and then the **ipconfig /registerdns** command on Maria's computer.
    E.   Install a 32-bit FTP client application on Gateway1.

Answer: D
Explanation: Maria has problems downloading from a particular site. Downloading from other sites is no problem. The most likely cause of this problem is an incorrect negative entry in the local DNS resolver cache. The **/ipconfig /flushdns** flushes and resets the contents of the DNS client resolver cache. Though not strictly necessary, we then use the **ipconfig/ registerdns** command to reinitiate a dynamic DNS registration of the client.

Note: The ipconfig /registerdns command provides you with a means to manually initiate a dynamic registration for the DNS names and IP addresses configured at a computer. This option can assist in troubleshooting a failed DNS name registration or in resolving a dynamic update problem between a client and the DNS server without requiring a client reboot.

Reference:
Windows 2000 Server documentation

Incorrect Answers:

A: Maria has no problem downloading from other sites. Gateway1 doesn't have to be reconfigured.

B: Maria has no problem downloading from other sites. There is no need to reconfigure Gateway1; in particular there is no need to configure a TCP/IP packet filter on Gateway1.

C: Configuring Maria's computer to use DNS2 as a secondary DNS server would not resolve this problem. DNS2 would only be used when DNS1 is unavailable.

This is DNS client problem, not a DNS server problem.

E: Maria has no problem downloading from other sites. Gateway1 doesn't have to be reconfigured. In particular adding a 32-bit FTP client application on Gateway1 would not help in any way whatsoever.

QUESTION NO: 244
You are the administrator of TestKing's network, which consists of a single segment. This segment includes 150 client computers and seven servers. Its network address is 172.30.10.0/24. One Windows 2000 Server computer is configured as a DHCP server with default settings. All client computers are DHCP clients.

Your DHCP server is configured with a single scope that has the characteristics shown in the following table.

DHCP scope	IP address range	IP address reservations	IP address exclusions
172.30.10./24	172.30.10.6 to 172.30.10.160	172.30.10.2 and 172.30.10.3	172.30.10.11 to 172.30.10.15

You need to add 90 new computers to this segment. You want the new computers to receive their IP configurations automatically, without adversely affecting any existing DHCP clients.

What should you do?

A.   Add a second scope that includes the IP address range of 172.30.10.161 to 172.30.10.254.

B.   Modify the existing scope properties to increase the upper end of the IP address range to 172.30.10.254.

C.   Delete the existing scope and create a new scope that includes the IP address range of 172.30.10.6 to 172.30.10.254. Add the appropriate reservations and exclusions.

D.   Add IP address reservations to the existing scope for each new computer. Use a unique IP address greater than 172.30.10.160 for each computer.

Answer: B

Explanation: We need support another 90 clients that use dynamic IP configuration. This can be accomplished by extending the upper limit of the existing scope from 172.30.10.160 to 173.30.10.254. This will extend the scope with 94 IP addresses. This is an adequate solution.

Reference:
Increasing the Number of IP Addresses on a Subnet (Q255999)
HOW TO: Install and Configure a DHCP Server in a Workgroup in Windows 2000 (Q301187)

Incorrect Answers:

A: Two different scopes on the same subnet is not a good idea. This would cause lease and release configuration problems.

C: There is no need to recreate the scope. That would require more administrative effort and it would affect the current DHCP clients as their leases would no longer be valid. Instead we simply extend the range of the current scope.

D: It would be awkward to use static IP addresses on all the 90 new client computers. It would require a huge administrative effort. It is better to let the new clients use dynamic IP configuration by extending the range of the current scope.

QUESTION NO: 245

You are the administrator of TestKing's network. The relevant portion of your network configuration is shown in the exhibit.
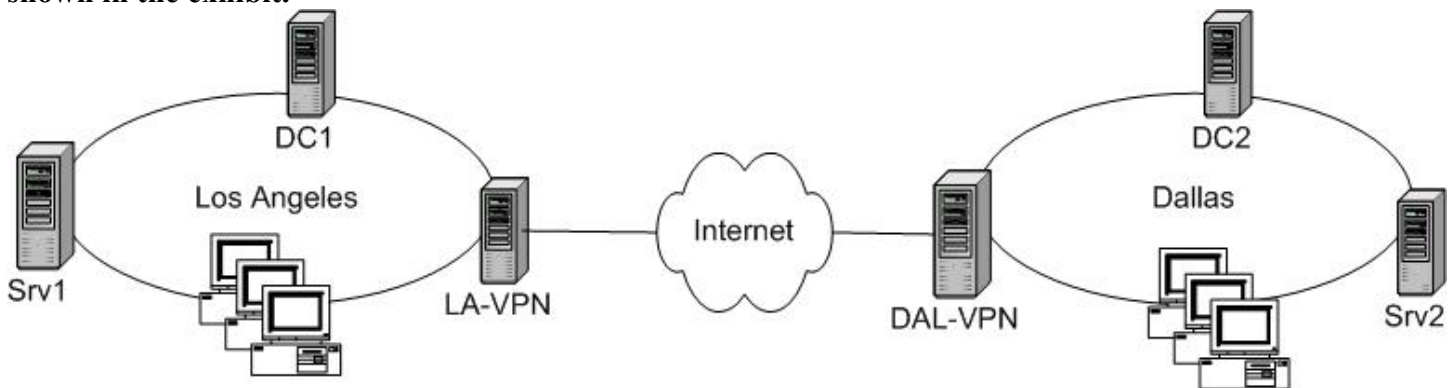
For communication between the Los Angeles and Dallas offices, you implement and configure two virtual private network (VPN) servers named LA-VPN and DAL-VPN. On each VPN server, you configure one L2TP port, one demand-dial VPN interface with default settings, and a Routing and Remote Access policy with an encryption setting of Strongest.

When you try to initiate a connection from Dallas to Los Angeles, you receive an error message stating that the remote computer does not support the required data encryption type.

How should you correct this problem?

    A.   Install and configure valid machine certificates on both VPN servers.
    B.   Configure the demand-dial interface on both VPN servers to use the Maximum strength encryption option on the connection.
    C.   Configure both VPN servers to use Windows authentication.
    D.   Configure both VPN servers to use RADIUS authentication.

Answer: A
Explanation: To implement encryption with L2TP we have to use IPSec. IPSec requires digital certificates. We must configure valid computer IPSec certificates on both VPN servers.

Incorrect Answers:
B: We already set the Routing and Remote Access polices on both VPN servers to **Strongest** Encryption. There is no need to change this setting.

        There is no such setting as **Maximum** strength encryption.

C: The communication should be initiated with digital certifications, not through Windows authentication.

D: There is no indication that any RADIUS server is used in either Los Angeles or Dallas. The communication should be initiated with digital certifications.

QUESTION NO: 246
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. You install Routing and Remote Access and the Network Address Translation protocol (NAT) on a Windows 2000 Server computer named NAT1. This server is used by internal users to access Internet resources.

Several mobile users require access to file and application resources on your internal network. You install Routing and Remote Access on another Windows 2000 Server computer named PPTP1 and configure PPTP virtual private network (VPN) ports for inbound access. The resulting network configuration is shown in the exhibit.
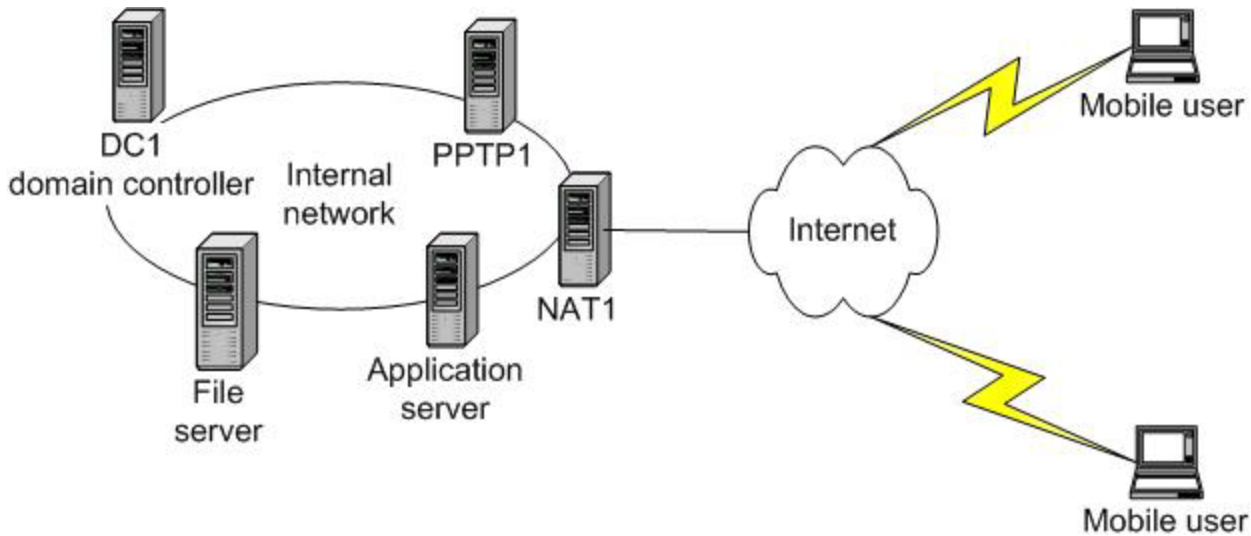
The mobile users now report that they cannot connect to the VPN server to access internal resources. How should you correct this problem?

A.   Configure NAT1 as your VPN server.
B.   Configure packet filters on NAT1 to allow PPTP traffic.
C.   Create a special port mapping on NAT1 for TCP port 1723 and IP protocol 47.
D.   Configure the PPTP Editor on NAT1 to allow access to PPTP1 by using TCP port 1723 and IP protocol 47.

Answer: A
Explanation:
NAT in Windows 2000 currently does not support incoming PPTP traffic from the external network(s) to an internal PPTP server behind the NAT server. We must therefore put the VPN server on NAT1.

Reference: Inbound PPTP Traffic and Windows 2000 Network Address Translation (Q263925)

Incorrect Answers:
B: We must use the PPTP Editor, not packet filters, to allow PPTP traffic.
C: It is not adequate to use port mappings. We must use the PPTP Editor.
D: NAT in Windows 2000 currently does not support incoming PPTP traffic from the external network(s) to an internal PPTP server behind the NAT server. Although you can create a special port mapping for TCP port 1723 to the PPTP server, there is no way to create a special port mapping for GRE traffic because it does not use TCP or UDP headers.

QUESTION NO: 247

You are the administrator of TestKing's network. The relevant portion of its configuration is shown in the exhibit.
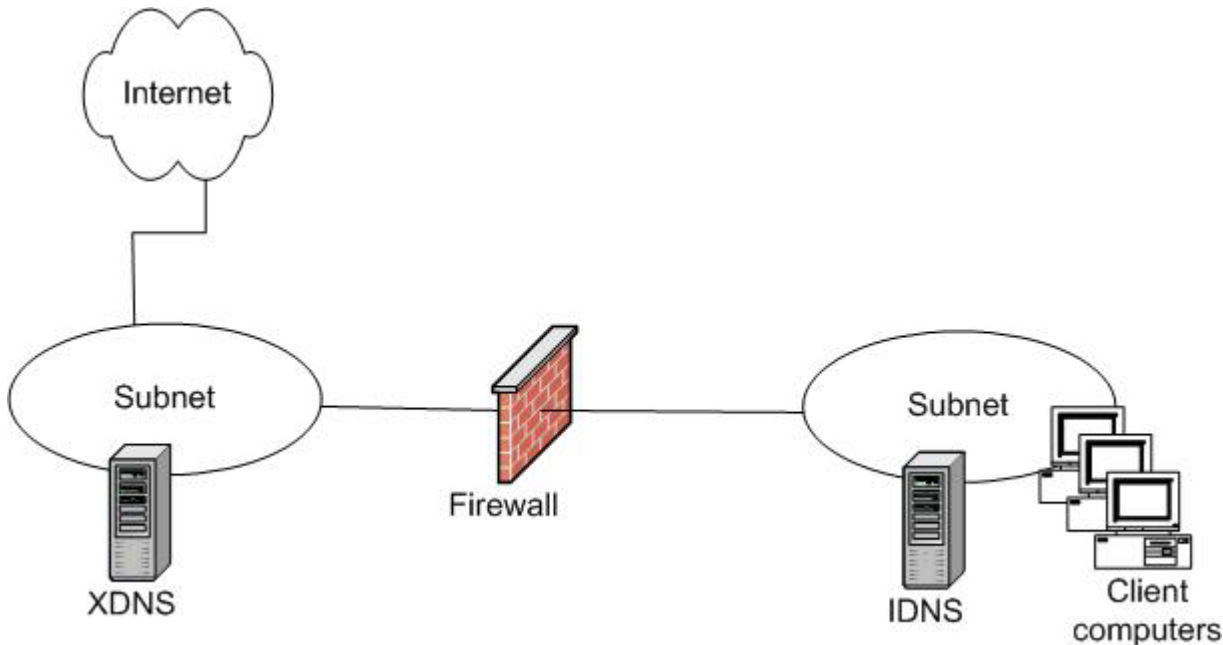
The client computers on your network are configured to use IDNS for DNS name resolution. IDNS and XDNS are configured with root hints to resolve DNS names on the Internet.

When users try to access certain Web sites on the Internet, they receive the following error message: "DNS server error." The problem does not occur for all Web sites, and it does not occur all the time.

On investigation, you discover that the problem occurs only when users try to access Web sites that are supported by multiple DNS servers located behind a firewall.

You need to configure your network to prevent this problem from occurring. What should you do?

    A.   On IDNS, copy the cache.dns file from the backup DNS folder to the main DNS folder. Stop and restart the DNS Server service on IDNS.
    B.   Configure IDNS to forward name resolution requests to XDNS:
    C.   Create resource records for the problem domain names in the zone file on IDNS.
    D.   Change the zone on IDNS to an Active Directory integrated zone.
    E.   Configure the client computers to use XDNS as a secondary DNS server.

Answer: B
Explanation: The IDNS DNS server has a problem communicating with some external DNS servers that are behind firewalls. The intercommunication must pass through two firewalls. To simplify the communication we configure IDNS to forward name resolution requests to XDNS. It would most likely decrease the name resolution problems.

Incorrect Answers:

A: The cache.dns file includes root server hints, but this is not a root zone problem. Replacing this file would not solve the problem at hand.

C: Manually creating resource records for the host names that fail is an ad hoc temporary solution. These records would have to be changed if the external web site changes the IP addresses. This solution is not practical.

D: There is not a problem with the local zones. It is a name resolution of an external host name that fails. Changing the zone on IDNS to Active Directory integrated would not solve this problem.

E: Clients are configured with a secondary DNS server for fault protection in case IDNS is not available. It is not a solution to the current problem. Instead, we should configure IDNS to forward requests to XDNS.

QUESTION NO: 248
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain with three sites. Each site has its own domain controller and its own DNS server, as shown in the exhibit.
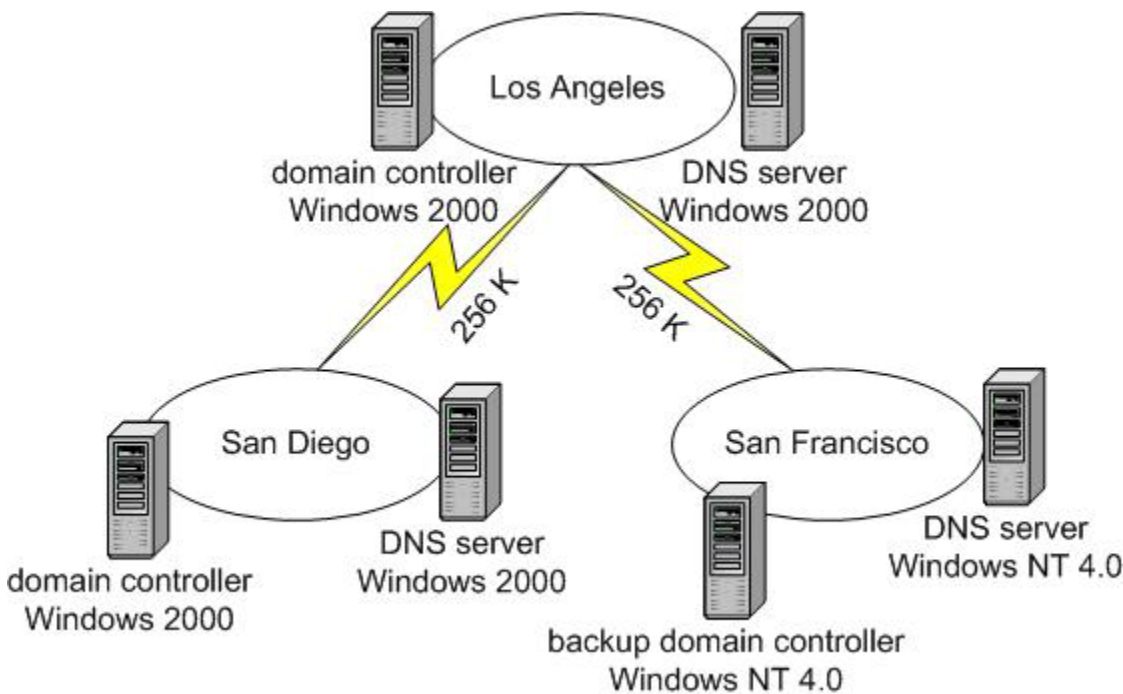
Each branch office includes 100 users. All client computers run either Windows NT Workstation 4.0 or Windows 98. The DNS server in Los Angeles hosts an Active Directory integrated zone. The DNS servers in San Diego and San Francisco host secondary zones that use the Active Directory integrated zone as the master zone.

Users in San Francisco report that access to resources in Los Angeles is frequently very slow. Users in San Diego do not report any problems. When you examine the utilization rates on the WAN links between the offices, you obtain the information shown in the following table.

Time	WAN link utilization from Los Angeles to San Diego	WAN link utilization from Los Angeles to San Francisco
8:00 A.M.	25%	75%
8:15 A.M.	30%	20%
8:30 A.M.	30%	15%
8:45 A.M.	35%	15%
9:00 A.M.	35%	70%
9:15 A.M.	30%	15%
9:30 A.M.	25%	15%

You need to minimize the utilization rates on the WAN link between Los Angeles and San Francisco. What should you do?

A.   Disable automatic notification of zone database changes on the DNS server in Los Angeles
B.   Upgrade all client computers to Windows 2000 Professional.
C.   Increase the refresh interval in the SOA (start of authority) record on the DNS server in Los Angeles.
D.   Upgrade the DNS server in San Francisco to Windows 2000 Server.
E.   Upgrade the backup domain controller in San Francisco to a Windows 2000 domain controller.

Answer: D
Explanation: The access of resources in Los Angeles is slow for the users in San Francisco and the network utilization on the Los Angeles/San Francisco WAN link must be reduced. Judging by the network utilization table the most likely cause of this is DNS zone transfers. The NT 4.0 DNS server at San Francisco does not support incremental zone updates, as the Windows 2000 server in San Diego does. We should therefore upgrade the DNS server at San Francisco to a Windows 2000 DNS server.

Incorrect Answers:
A: Zone changes must be transferred to all DNS servers in order for the DNS servers to have accurate host name records. Disabling the notification of zone database changes at Los Angeles would minimize zone transfer traffic but the resource records at the DNS server at San Diego and San Francisco would not be up to date.

B: Upgrading the clients would not reduce WAN utilization. Instead we must upgrade the DNS server.

C: Decreasing the refresh interval would reduce the number of zone transfers, but at the same time DNS zones at San Diego and San Francisco would be less accurate. This is not the best solution.

E: It is not necessary to upgrade the domain controller at San Francisco to a Windows 2000 domain controller. We should instead upgrade the DNS server.

QUESTION NO: 249
You are the administrator of TestKing's network, which uses TCP/IP as its only protocol. The network uses the private address space of 172.16.0.0/16.

Your company projects rapid growth during the next three years. To reduce the risk of network saturation, you decide to subnet the network. You will eventually need to accommodate a maximum of 17 subnets. Each subnet will include a maximum of 1,200 hosts.

Which subnet mask should you configure to meet both your current needs and your projected needs?

    A.   255.255.224.0
    B.   255.255.240.0
    C.   255.255.248.0
    D.   255.255.254.0
    E.   255.255.255.0

Answer: C
Explanation: We need to support 1,200 hosts. We will need at least 11 bits for the hosts, since $2^{10}=1024 < 1200 < 2^{11}=2048$.
We need to support 17 subnets. We will need at least 5 bits for the subnets, since $2^4=16 < 17 < 2^5=32$.
This solution is working since we are going to subnet the network 172.16.0.0/16. We can use the 16 hosts bit to make 32 subnets (only 30 available) using 5 bits and 2048 hosts (only 2046 available) using 11 bits.

We calculate the third octet in the subnet mask which uses the highest five bits: 11111000 binary which equals 248 in decimal (128+64+32+16+8). Therefore the 255.255.248.0 subnet mask is the correct answer.

Incorrect Answers:
A: The 255.255.224.0 subnet mask uses only 3 bits (224=128+64+32) for the subnets. Only 8 (more precisely only 6) subnets could be used, but we need 17 subnets.
B: The 255.255.240.0 subnet mask uses only 4 bits (240=128+64+32+16) for the subnets. Only 16 (more precisely only 14) subnets could be used, but we need 17 subnets.
D: The 255.255.254.0 subnet mask only leaves 9 bits for hosts. Only 512 (more precisely only 510) hosts could be used, but we need to accommodate for 1,200 hosts.
E: The 255.255.254.0 subnet mask only leaves 8 bits for hosts. Only 256 (more precisely only 254) hosts could be used, but we need to accommodate for 1,200 hosts.

QUESTION NO: 250
You are the administrator of TestKing's network. The relevant portion of its configuration is shown in the exhibit.
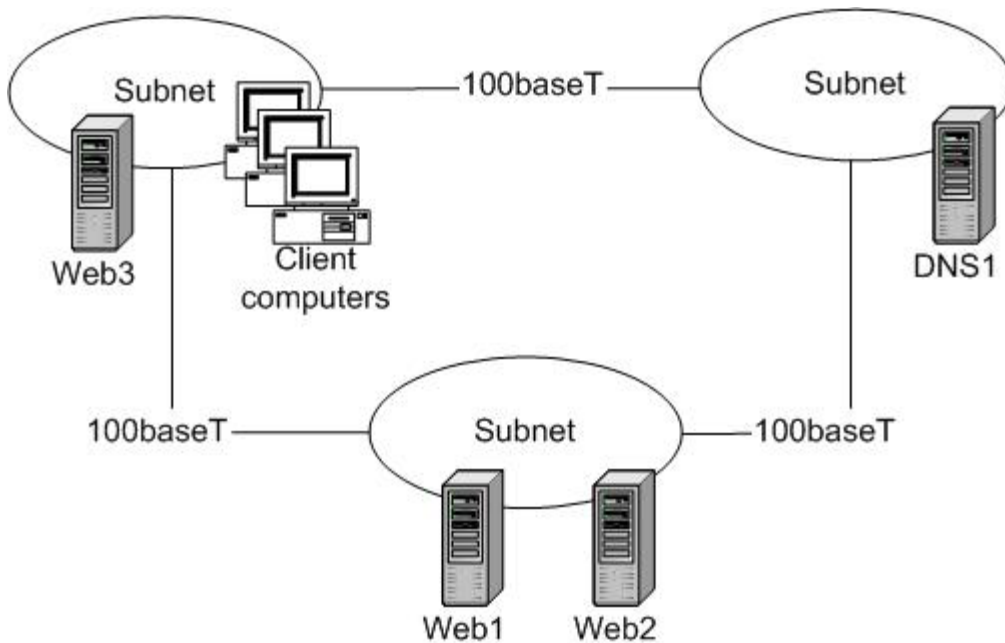
Web1, Web2, and Web3 are Windows 2000 Server computers running a Web application named FinanceApp. All three servers contain identical content. The client computers are configured to use DNS1 for name resolution. DNS1 is configured with a single standard primary zone. DNS1 is also configured to distribute name resolution requests for the FinanceApp equally across Web1, Web2, and Web3.

Users report that access to FinanceApp is very slow. On investigation, you discover that the W3SVC log files on Web1 and Web2 are empty. The W3SVC log files on Web3 are very large.

You need to improve response time to FinanceApp. What should you do?

    A.   Configure DNS1 to allow dynamic updates.
    B.   Ensure that round robin is enabled on DNS1.
    C.   Disable the LocalNetPriority setting on DNS1.
    D.   Promote DNS1 to domain controller and convert the DNS zone to an Active Directory integrated zone.

Answer: C
Explanation: By default, the Microsoft DNS server gives priority to the "closest" A record to the client's IP address when there are multiple A records for a name. This is designed so that the client application will attempt to connect to the closest (and fastest) IP available. This overrides Round-robin and the DNS server returns Host resources that are local to the requestor instead of using round robin. However round robin can be enabled by disabling the LocalNetPriority setting on the DNS server.
In our scenario the clients will only use the web server located on their own subnet, Web3, unless we disable the LocalNetPriority setting.

Note 1: The simplest load-balancing method uses DNS round-robin. When round-robin is enabled the DNS server rotates and reorders a list of multiple host (A) resource records if a queried host name is for a computer configured with multiple IP addresses.

Note 2: **Enable DNS round robin resolution in an environment that uses LocalNetPriority**
1. Start the registry editor (regedit.exe)
2. Move to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters
3. From the Edit menu select New - DWORD Value
4. Enter a name of LocalNetPriority and press Enter
5. Double click the new value and set to 0 to disable LocalNetPriority and re-enable round robin. Click OK
6. Close the registry editor
7. Stop and restart the DNS service

Reference:
Microsoft DNS Server Registry Parameters, Part 2 of 3 (Q198409)

Incorrect Answers:
A: Dynamic updates concerns DNS updates from DHCP clients. The Web servers are not DHCP clients. Allowing dynamic updates would not solve the problem at hand.
B: The scenario text states that DNS1 is already configured to distribute name resolution requests for the FinanceApp equally across Web1, Web2, and Web3. By default Round-Robin is enabled. Enabling Round-Robin is therefore not the solution to this problem.
D: Round-robin doesn't require Active Directory integrated zones. Converting the DNS zone to an Active Directory integrated zone will not address the current problem.

QUESTION NO: 251
You are the administrator of TestKing's network. The network includes one DNS server running UNIX, three file servers running NetWare 5.0, two servers running Windows 2000 Server, and 250 client computers. The client computers run either Windows 2000 Professional or Windows NT Workstation 4.0.

Currently, all computers on your network use TCP/IP as their only network protocol, and all have static IP addresses. All client computers have the address of the DNS server statically entered.

You install DHCP and DNS on a new computer named DD1, which runs Windows 2000 Server. You then decommission the UNIX DNS server. You configure DD1 to require secure dynamic updates. You also configure DD1 so it always DNS records for all DHCP clients. You configure the DHCP scope to assign DD1 as the DNS server for all client computers. All servers continue to use static IP addresses.

Users now report they cannot access resources located on the NetWare file servers. However, they can access resources located on the Windows 2000 computers.

You need to ensure that all users can access resources on the NetWare file servers. What should you do?

    A.   Configure DD1 so it does not require secure dynamic updates.
    B.   Configure the NetWare file servers to point to DD1 for DNS name resolution.
    C.   On DD1, create CNAME (canonical name) records that point to the NetWare file servers.
   D.   On DD1, create A (host) records that point to the NetWare file servers.

Answer: D
Explanation: We must manually add A (Host) records for the NetWare file servers. NetWare computers would not be able to use dynamic DNS and register themselves in the DNS zone.

Incorrect Answers:
A: The NetWare file servers would not be able to register themselves dynamically under any circumstances. Removing the requirement for secure dynamic updates would not enable the NetWare file servers to register in the DNS zone.
B: The Windows 2000 clients must be able to access the NetWare file servers. We don't have to change how the NetWare file servers uses name resolution.
C: Canonical name (CNAME) records enable you to associate more than one host name with an IP address. This is sometimes referred to as aliasing. In this scenario, however, we don't have any records for the NetWare file servers in the DNS zone so adding CNAME records for them would be pointless.

QUESTION NO: 252
You are the administrator of TestKing's network. The relevant portion of its configuration is shown in the exhibit.
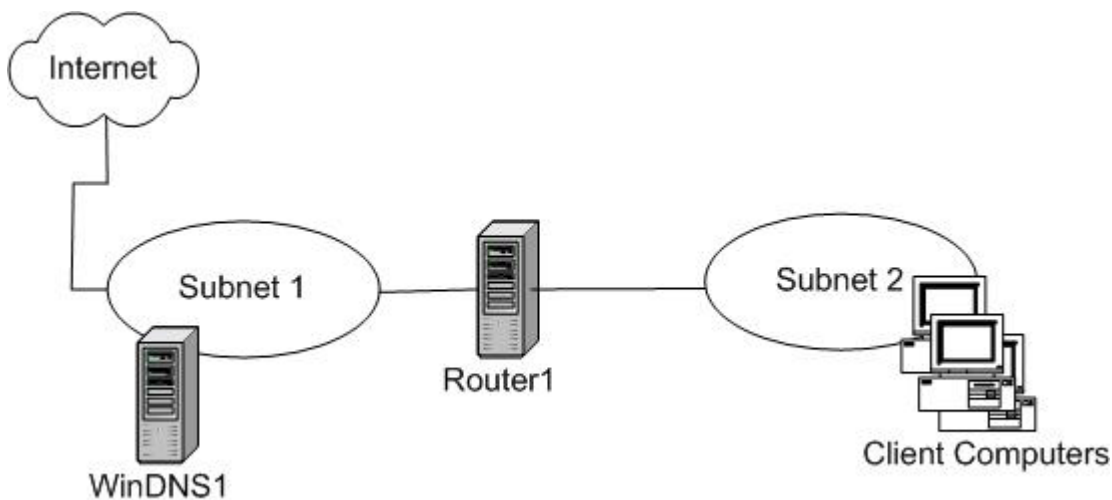
WinDNS1 runs Windows 2000 Server and the DNS Server service. Router1 runs Windows 2000 Server and Routing and Remote Access. All client computers run Windows 2000 Professional.

You configure TCP/IP filters on Router1 so that users can access Web sites through Router1.

You can use the ping command to test TCP/IP connectivity between your client computers and your network servers. However, when you ping WinDNS1, your requests times out.

You need to use the ping command to verify TCP/IP connectivity between client computers and WinDNS1. Which action should you perform on Router1?

    A.   Create a static TCP/IP route that directs packets from your client computer to WinDNS1.
    B.   Create a static TCP/IP route that directs packets from WinDNS1 to your client computer.
    C.   Configure an additional TCP/IP filter to allow TCP port 2.
    D.   Configure an additional TCP/IP filter to allow ICMP.

Answer: D
Explanation: We have configured Router1 with TCP/IP filters to allow access to Web sites. The PING utility uses the ICMP protocol, which isn't required in usual Web traffic. We need to add a filter which allows ICMP traffic in order to make PING work.

Incorrect Answers:
A: We should first allow ICMP traffic.
B: We should first allow ICMP traffic.
C: We should create a filter that allows ICMP, not a filter that allows TCP port 2.

QUESTION NO: 253
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The relevant portion of its configuration is shown in the exhibit.
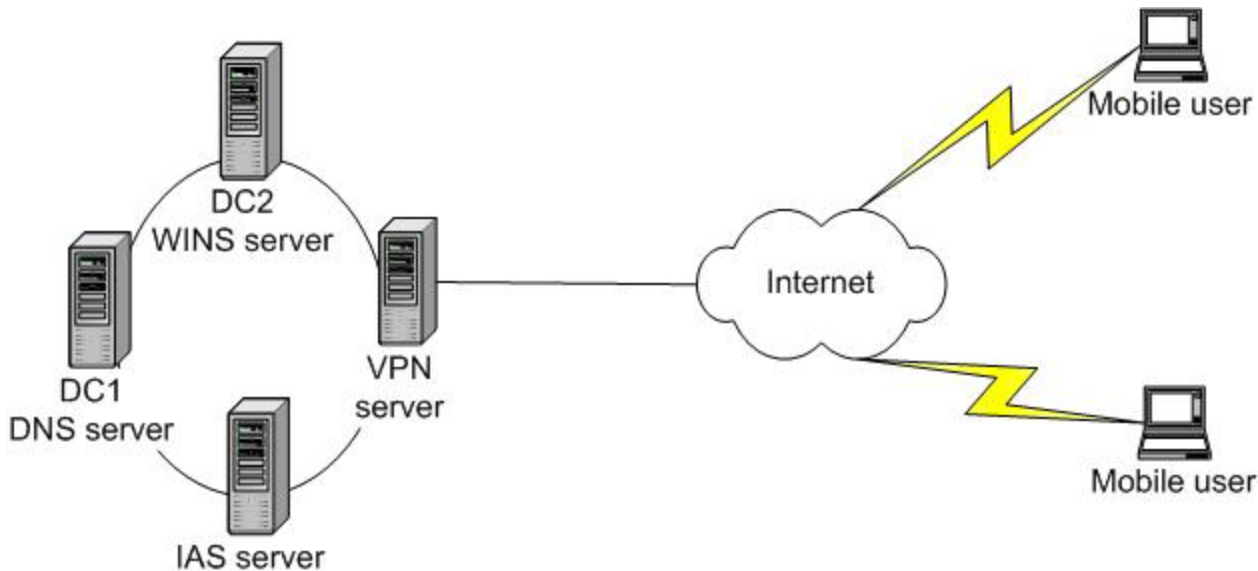
Several mobile users require access to network resources when they are traveling. You install a third-party virtual private network (VPN) server to provide user connectivity to the network. You require all VPN users to be authenticated by the domain. You install the Internet Authentication Service (IAS) on a member server in the domain and configure the VPN server as a RADIUS client.

The mobile users now report that they cannot access the network from remote locations. They receive this error message: "Unknown user name or bad password."

You verify that these users have valid accounts in the domain and that they are entering their user names and passwords correctly. When you view the event logs on the IAS server you find event messages that state "The current configuration supports only local user accounts."

How should you correct this problem?

    A.   Promote the IAS server to be a domain controller in the domain.
    B.   Add the IAS server to the RAS and IAS Servers domain local group.
    C.   Change the RADIUS client configuration to use the RADIUS standard client-vendor type.
    D.   Set the realm replacement rules on the IAS server to add the domain to the user name for authentication.

Answer: B
Explanation: The error message "The current configuration supports only local user accounts." indicates that IAS is set up to authenticate against the local SAM, but the user is not a member of the local user database. To resolve this problem we must add the IAS server to Active Directory. Or more precisely, we must enable the IAS server to read user objects in Active Directory. This can be accomplished by adding the IAS server to the RAS and IAS Servers domain local group.

Note: To add the IAS server to a domain:

1. Log on to the server using domain administrator credentials.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the console tree, select **Users**.
4. In the details pane, right-click **RAS and IAS Servers**, and then click **Properties**.
5. In the **RAS and IAS Servers Properties** dialog box, on the **Members** tab, add each of the IAS servers.

Reference: Windows 2000 Server Resource Kit, Internet Authentication Service, Troubleshooting IAS Installation

Incorrect Answers:
A: Promoting the IAS server to domain controller would not, by itself, register the IAS server in the Active Directory. It could, however, be a security risk.

C: This isn't a client configuration problem. We must add the IAS server to the Active Directory.

D: Realm replacement rules are used to map domain names to other domain names. They cannot, however, give the remote clients remote access in this scenario.

QUESTION NO: 254
You are the network administrator for your company, which operates a main office and one branch office. The main office contains a Windows 2000 computer named RAS1, which runs Routing and Remote Access. The branch office contains a Windows 2000 Server computer named BR1, which you configure as a demand-dial router to RAS1. Both servers use RIP in auto-static update mode.

Users at the branch office need to connect to the main office a maximum of three times each day. Every time they connect, they provide updates for an inventory application hosted on a database server named DB1.

Branch office users now report that they can connect to the main office, but they cannot access DB1. You need to correct this problem with the least possible administrative effort.

What should you do?

A. On RAS1, disable RIP. On the external interface of BR1, enable the OSPF protocol.
B. On the demand-dial interface on BR1, disable RIP. On the external interface on RAS1, enable the OSPF protocol.
C. On the demand-dial interface on BR1, disable RIP. Add the appropriate static routes to BR1.
D. While an active connection links RAS1 and BR1, update the routes for the auto-static update mode on both servers.

Answer: D

Explanation: For demand-dial interfaces, Auto-static update is the default. When you use auto-static updates, the router does not send any regular router update announcements. You must manually send a request to other routers, asking for a copy of their routing tables. This information is stored in the local routing table, in entries marked as auto-static routes, until the interface goes down or another update is requested.

In this scenario we are able to connect, but we are unable to access the remote server. We must request an update of the routing tables while an active connection between the servers exists.

Reference:
How to Implement RIP Over RRAS in Windows 2000 (Q241545)
RIP and OSPF Do Not Start Dial On Demand Connections (Q235492)

Incorrect Answers:
A: There is no need disable RIP or to enable OSPF:
B: There is no need disable RIP or to enable OSPF:
C: There is no need to disable RIP; instead we just update the routes on bother servers.

QUESTION NO: 255
You are the administrator of TestKing's network, which currently consists of a single Token Ring network segment. You reconfigure the network to consist of two separate network segments. The relevant portion of the resulting configuration is shown in the exhibit.
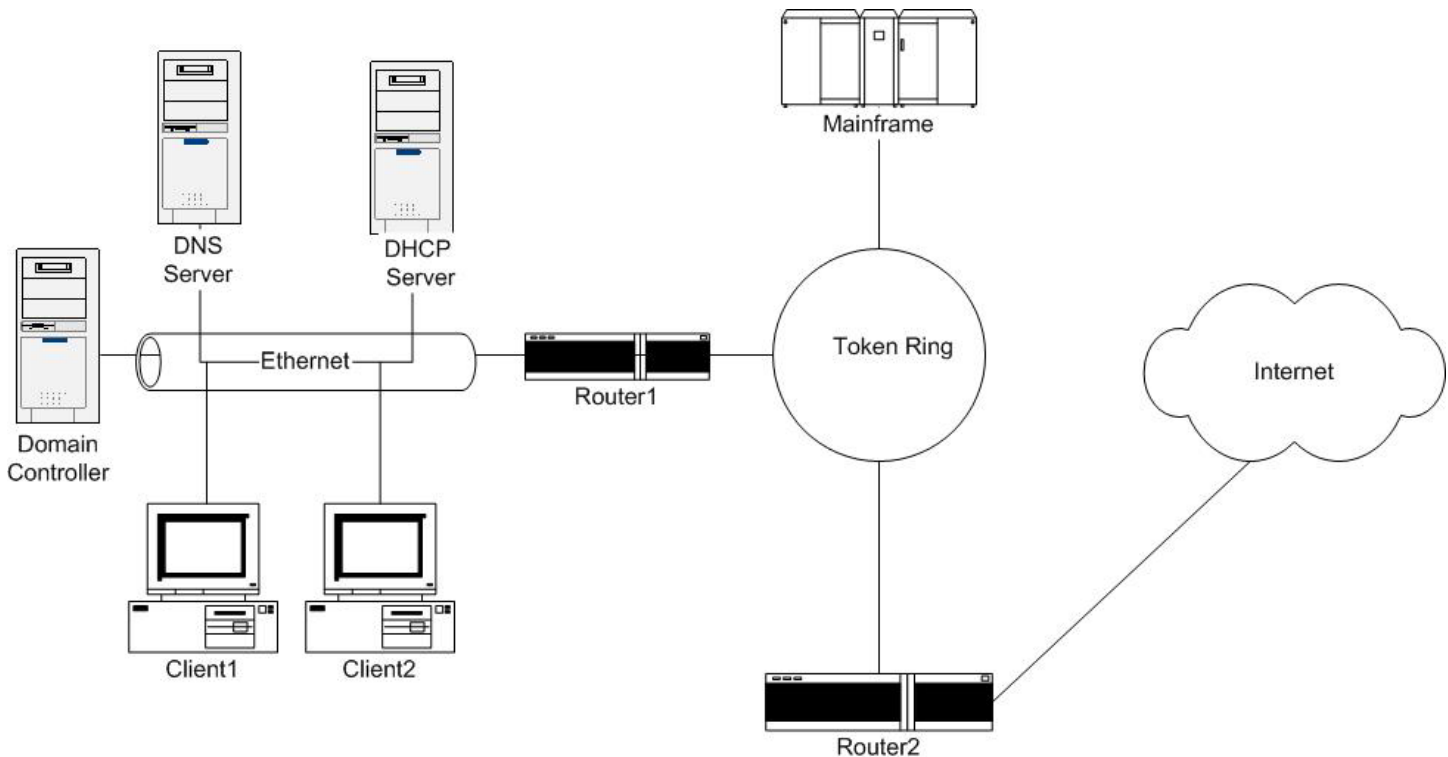
All client computers are DHCP clients, and all use third-party TN3270 terminal emulation client software to connect to the mainframe computer. All servers have static IP addresses.

Users now report that they cannot access resources located on the mainframe computer or the Internet. From Client1, you ping a well-known Internet host. You receive the following error message: "Destination host unreachable."

You must ensure that client computers can access resources on the Internet and the mainframe computer. What should you do?

A.   Change the Ethernet segment to Token Ring.
B.   Configure the default gateway on Router1 to be Router2.
C.   Configure the default gateway on Router2 to be Router1.
D.   For DHCP clients on the Ethernet segment, configure a DHCP scope Default Gateway option to be Router1.
E.   Configure a DHCP global DNS option to be a DNS server on the Internet. Configure a Hosts file entry for the mainframe computer on each client computer.

Answer: D
Explanation: The computers on the Ethernet segment are not able access resources outside their segment. Most likely the default gateway setting on the computers is incorrect. We can solve this problem by configuring the Default Gateway option to be Router1 in the DHCP scope option.

Incorrect Answers:

A: There is no need to change the Ethernet segment to Token Ring.

B: Configuring the default gateway setting on Router1 will not help the users to access the mainframe computer.

C: The users are unable to reach Router2. Reconfiguring Router2 will not help.

E: We should not primarily use an external DNS server. We should use the local DNS server. The local DNS server could be configured to forward name resolution to an external DNS server if necessary.

QUESTION NO: 256
You are the administrator of TestKing's network, which includes three subnets. Each subnet contains 200 Windows 2000 Professional computers and five Windows 2000 Server computers. One Windows 2000 Server computer in one subnet runs the DNS Server service. The DNS server is configured to allow dynamic updates. All computers on the network have static IP addresses.

You add two UNIX servers named IW1 and IW2 to the network. Both servers host identical content for your internal Web site.

When you try to access this internal Web site from your client computer, your Web browser displays this message: "Can't find server or DNS error." However, when you enter the IP addresses of the two Web servers in your browser, you can view the Web site.

You need to ensure that you can access each internal Web server by its name. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

    A.   Add one A (host) record to the DNS server for IW1. Add another for IW2.
    B.   Add one CNAME (canonical name) record named WWW to the DNS server for IW1. Add another CNAME record named WWW for IW2.
    C.   Disable dynamic updates on the DNS server.
    D.   Run the **ipconfig /flushdns** command on your client computer.
    E.   Run the **ipconfig /registerdns** command on your client computer.

Answer: A, D
Explanation:
A: The UNIX servers cannot register dynamically in the DNS zone on the Windows 2000 DNS server. We must manually add their A (Host) records to the zone.

D: There is an incorrect negative entry in the local DNS resolver cache for IW1 and IW2, since you unsuccessfully tried to connect to them. The **/ipconfig /flushdns** flushes and resets the contents of the DNS client resolver cache and enables you to connect to IW1 and IW2.

Incorrect Answers:

B: We should add A (Host) records, not CNAME (canonical name) records to the zone. CNAME records are used to define aliases for existing A (Host) records, but we have no A (Host) records for IW1 or IW2 yet.

C: IW1 and IW2 cannot register themselves dynamically in the DNS zone. Disabling dynamic updates would prevent Windows computers from registering themselves. This would not solve any problems in this scenario.

E: There is no need to register your client computer in the DNS zone. The problem is with the A (host) records for IW1 and IW2. Reregistering your client computer will not help.

QUESTION NO: 257
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The network includes seven servers running Windows 2000 Server and 300 client computers running Windows 2000 Professional. Your primary DNS server is Server1, which has a persistent connection to TestKing's Internet service provider (ISP).

Your assistant, Lillianne, configures the Network Address Translation protocol (NAT) on Server1 to provide shared-connection Internet access for users who require it. However, users now report that they can no longer access TestKing's internal Web server. You also discover that internal DNS queries are no longer resolving.

The application event log on Server1 shows the following event messages.

```
Event ID: 407
Source: DNS
Description: DNS server could not bind a datagram socket to 192.168.0.1.
The data is the error.

Event ID: 408
Source: DNS
Description: DNS Server could not open socket for address (192.168.0.1).
Verify that this is a valid IP address on this machine. If it is NOT valid
use the Interfaces dialog under Server Properties in the DNS Manager to
remove it from the list of IP interfaces. Then stop and restart then DNS
server. (If this was the only IP interface on this machine and the DNS
server may not have started as a result of this error. In that case remove
the DNS\Parameters\ListenAddress value in the services section of the
registry and restart.) If this is a valid IP address for this machine,
make sure that no other applications (e.g., another DNS server) is running
that would attempt to use the DNS port.
```

You need to provide the appropriate Internet Access to company users. Your solution should involve the least possible administrative effort and the fewest possible changes to your current network configuration.

What should you do?

A. Remove the 192.168.0.1 interface from the Server Properties page in the DNS Manager. Stop and restart Server1.
B. Remove NAT from Server1. Configure Server1 to use Internet Connection Sharing.
C. Remove NAT from Server1. Configure NAT on a different server in the network.
D. Disable the DNS proxy functions in NAT.

Answer: C
Explanation: This problem can occur when you have a NAT server that also is used as a DNS server. NAT has a DNS Proxy setting that enables DHCP clients to direct DNS queries to the NAT server. The client DNS queries are then forwarded to the NAT server's configured DNS server. The DNS Proxy and the DNS Server service cannot coexist on the same host if the host is using the same interface and IP address with the default settings.

There are three methods to overcome this problem:
1. Reconfigure the DNS server service not to listen on the internal address.
2. Install NAT and DNS on different servers. This is the solution in this scenario.
3. Use the DHCP server Service in NAT, NOT the DHCP Allocator and DNS Proxy.

Reference: JSI Tip 3284, Your DNS Event Log reports Event Ids 407 and 408

Incorrect Answers:
A: We could configure the DNS server service not to listen to the internal address, 192.168.0.1. This would solve the problem, but we cannot, however, remove the 192.168.0.1 interface. The DNS server must still be able to function as a DNS server for the internal client computers.
B: Internet Connection Sharing cannot be used in a network with a DNS server.
D: Just disabling the DNS proxy function in NAT is not enough to solve the problem.

QUESTION NO: 258
You are the network administrator for Contoso Ltd. Your network consists of a single Active Directory domain named contoso.com. The network includes four Active Directory sites, one at your main office and one at each of three branch offices. Each branch office is a separate OU within the contoso.com domain, and each one has approximately 500 users. The relevant portion of your network configuration is shown in the exhibit.
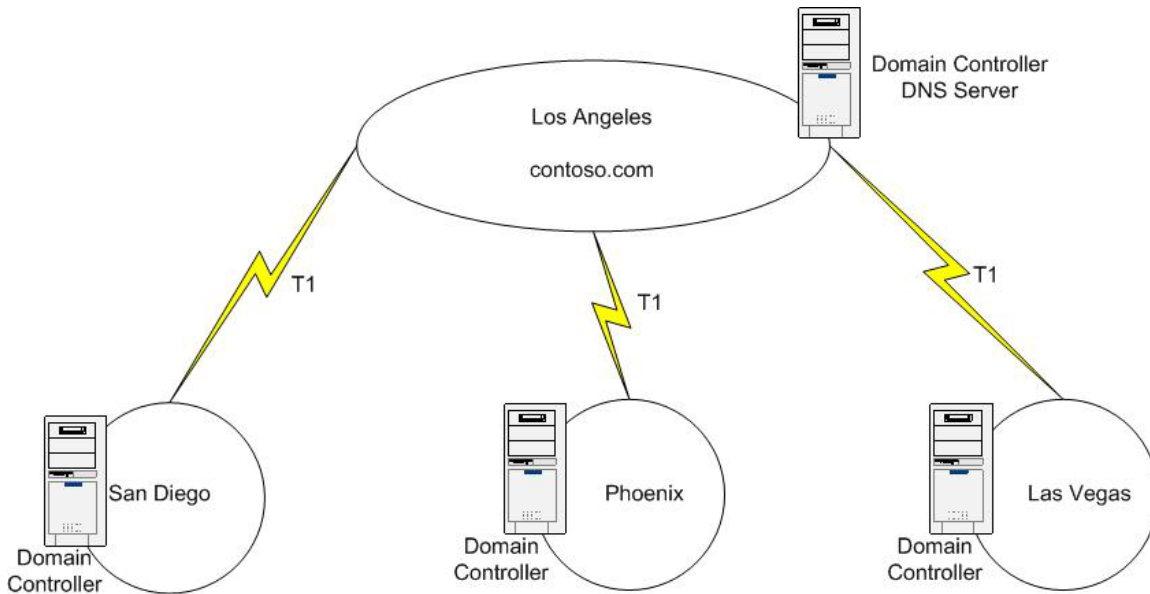
Users at the branch offices report extremely slow response times when they try to access local network resources. You monitor network traffic and discover that each request for name resolution takes several minutes.

You need to improve access times and minimize the amount of T1 bandwidth used by name resolution. Your solution must involve the least possible administrative effort.

What should you do?

    A.   Install and configure one caching-only DNS server in each branch office
    B.   Install and configure one WINS server in each branch office to provide name resolution
    C.   Install and configure one DNS server in each branch office. Create an Active Directory integrated zone within contoso.com
    D.   Replace the branch office OUs with child domains. Configure DNS servers in each branch office with Active Directory integrated zones for the domain.

Answer: C
Explanation: In the scenario all name resolution traffic crosses the WAN links. This makes the name resolution slow. The goal is to set up the network so that the clients use a local DNS server for name resolution. By creating an Active Directory zone within contoso.com and putting a DNS server in each branch office. This will result in clients using local DNS servers for name resolution and will minimize the amount of T1 bandwidth used by name resolution. It will also require minimal administrative effort.

Incorrect Answers:
A: Caching-only DNS servers are the recommended solution on slow connections, for example 128 Kbps ISDN lines.
B: DNS, not WINS, is used for name resolution in a Windows 2000 domain

D: By replacing the OUs with child domains, and configuring DNS servers with Active Directory integrated zones for the domains we will ensure that the clients will use the local DNS servers for name resolution and that zone transfers will be fast; but there would be considerable administrative effort to set up the child domains, and the scenario calls for minimal administrative effort.

QUESTION NO: 259
You are the administrator of TestKing's network. The relevant portion of is configuration is shown in the exhibit.
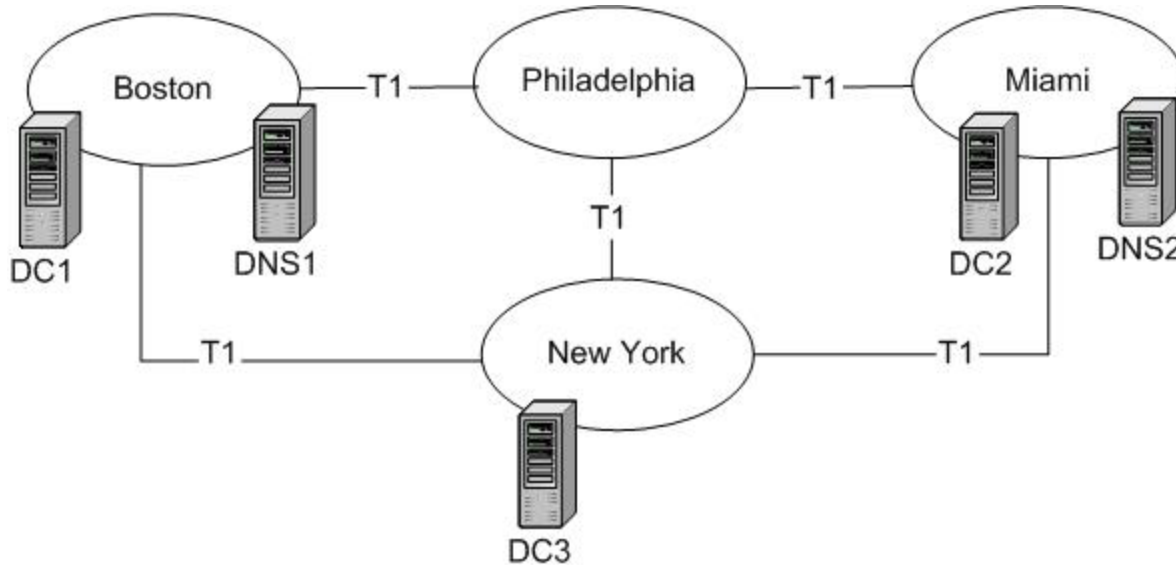
The network consists of a single Windows 2000 domain, and it includes three domain controllers named DC1, DC2, and DC3. The network also includes two DNS servers named DNS1 and DNS2.

DNS1 hosts a standard primary zone and DNS2 hosts a standard secondary zone. Both servers are members of the Windows 2000 domain.

Users in New York and Philadelphia report that access to some network resources is extremely slow. You discover that name resolution requests in these locations sometimes take longer than one minute to process.
Company management expects to add more than 150 new users to these locations in the next few months. You are concerned that the existing DNS servers will not be adequate.

You need to improve response times for name resolution requests in New York and Philadelphia. You must take into consideration the expected growth in these locations. You must also ensure that the DNS servers do not have a single point of failure.

What should you do?

A.   Install one new DNS server in New York and another in Philadelphia.

Configure both servers with a standard secondary zone.
B.   Install a new domain controller in Philadelphia. Remove the DNS Server service from DNS1 and DNS2. Install the DNS Server service on all four domain controllers. Create an Active Directory integrated zone.
C.   Install one caching-only DNS server in New York and another in Philadelphia. Configure both servers to forward name resolution requests to DNS1 and DNS2.
D.   Install a caching-only DNS server in Philadelphia. Remove the DNS Server service from DNS1 and DNS2. Install the DNS Server service on DC1. Create an Active Directory integrated zone.

Answer: B
Explanation: We should simply install an Active Integrated DNS zone at each location. All four DNS servers would be able to update the DNS zone, so we would not have a single point of failure. The local computers could be configured to use their local DNS server for name resolution. This would reduce network utilization and increase performance.

Incorrect Answers:
A: With one DNS server hosting a primary a zone and three DNS servers hosting secondary zones, the DNS server with the primary zone is a single point of failure.

C: Installing caching-only servers in New York and Philadelphia would improve name resolution somewhat in these locations. Caching-only servers are best used in remote locations over slow WAN links, typically 128 Kbps or slower. However, the DNS server hosting the primary zone would be a single point of failure.

D: With only one single DNS server hosting the Active Directory zone, we would have a single point of failure. To reduce network traffic we should have one DNS server at each location.

QUESTION NO: 260
You are the network administrator for Fabrikam Inc. Your network includes one Windows 2000 Server computer running Routing and Remote Access, which is used by company employees to dial in to the network. According to company policies, members of the Managers and Sales groups are the only users who are allowed to access the network after 8:00 P.M., seven days a week.

Your current remote access policies are summarized in the following table.

Policy	Order
Weekday 6:00 A.M. – 8:00 P.M.: Allow	1
Managers: Allow	2
Sales: Allow	3
Weekday 8:00 P.M. – 6.00 A.M.: Deny	4
Weekend: Deny	5

Your company acquires a subsidiary named **Wingtip Toys**, which employs 500 users. You add the management and sales staff at **Wingtip Toys** to the appropriate domain groups in the **Fabrikam Inc.** domain.

Currently, users at **Wingtip Toys** are approved for remote network access only between 6 A.M. and 8 P.M., Monday through Friday. However, you anticipate that the Managers and Sales groups at **Wingtip Toys** will be approved for evening and weekend access within three weeks. The members of the Sales group will be dialing in from a variety of locations, both remote and on-site.

You need to reconfigure your remote access policies to accommodate the new users, without affecting access for users at **Fabrikam Inc.** Your solution must take into account the expected changes in access policy, and it must involve the least possible administrative effort.

What should you do?

    A.   Create a policy named Calling from Subsidiary. Deny and place it directly above policy 2.
    B.   Create a policy named Calling from Subsidiary: Deny and place it directly above policy 5.
    C.   Create a Subsidiary group for all subsidiary employees. Create a policy named Subsidiary. Deny and place it directly above policy 4.
    D.   Create a Subsidiary group for all subsidiary employees. Create a policy named Subsidiary. Deny and place it directly above policy 2.

Answer: D
Explanation: We must make sure that the new users from Wingtip Toys only get access between 6.A.M. and 8 P.M. even though some of them already belong to the Managers and Sales groups. First we must create a new group and place all of the users from Wingtip Toys into this group. Then we must create a new policy which applies only the members of this new group (this isn't explicitly stated in any alternative – we must take it for granted). Furthermore, we must place this policy before the policies that allow Managers and Sales unlimited access. We must place the policy directly above policy 2.

Note: Access policies are applied one at a time in order. If an access policy does not apply the next access policy is processed. If an access policy matches then access is either granted or denied and no further access policies are processed. Finally, if no access policy matches the access will not be granted.

Incorrect Answers:
A: We must add a group condition to the policy so that it only applies to users from Wingtip Toys.
B: We must add a group condition to the policy so that it only applies to users from Wingtip Toys. The policy should not be placed after policy 2 and policy 3.
C: If we place the new policy after policy 2 and policy 3 the users from Wingtip Toys that are members of either Managers of Sales would get 7/24 access to the network, since policy 2 or policy 3 would apply to them. The new deny policy must be placed above policy 2.

QUESTION NO: 261
You are the administrator of TestKing's network. One segment includes 100 desktop computers and 50 portable computers. All 150 client computers run Windows 2000 Professional and are DHCP clients. The portable computers are typically in use off-site.

The scope for the segment has the characteristics shown in the following table.

IP address range	Lease duration	Conflict detection attempts	Enable dynamic update of DNS records
172.16.10.51 to 172.16.10.250	8 days	0	Yes

You disconnect the 100 desktop computers and replace them with new hardware. When you connect the new computers to the segment, half of them can communicate with other hosts on the local network and on remote networks. The other half cannot communicate with any hosts at all.

You need to enable all the new computers to communicate with remote networks. What are two possible ways for you to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

A.   Disable Automatic Private IP Addressing (APIPA) on the new computers.
B.   On each computer that is unable to communicate with remote networks, run the **ipconfig /renew** command.
C.   Delete all the existing leases for the scope. Increase the setting for conflict detection attempts to **1**.
D.   Temporarily reduce the lease duration for the scope to one minute.
       Reset the duration to eight days after one minute has elapsed.
E.   Compile a list of the IP addresses that are now being used successfully by the new computers and the portable computers. For any IP addresses that do not appear on the list, delete the current leases in the scope.

Answer: C, E
Explanation: The DHCP scope contains 200 IP addresses. 150 IP addresses are leased and 100 of these are leased by desktop computers that have been replaced. We then add 100 new computers; only 50 of these new computers are able to receive IP leases. We must be able to use the IP addresses leased by the removed computers. This can be accomplished by:
**C:**   Deleting all existing leases, and increasing the conflict detection attempts from the default value of 0 to 1, which will make the transition smoother.
E: Though it would be a daunting administrative task, we could check which IP addresses are leased by the removed computers, and delete the leases from the scope.

Incorrect Answers:

A: Disabling APIPA would prevent the clients from using APIPA. APIPA would enable the clients with no leases to communicate with each other. Disabling APIPA would not help in any way in this scenario.

B: All IP addresses in the DHCP scope are already leased. Forcing a new lease from the clients with the **ipconfig /renew** would not be successful since there are no IP addresses to lease.

D: The current leases would not be affected by a change of lease duration. Only new leases would be affected.

QUESTION NO: 262
You are the administrator of TestKing's network. The relevant portion of its configuration is shown in the exhibit.
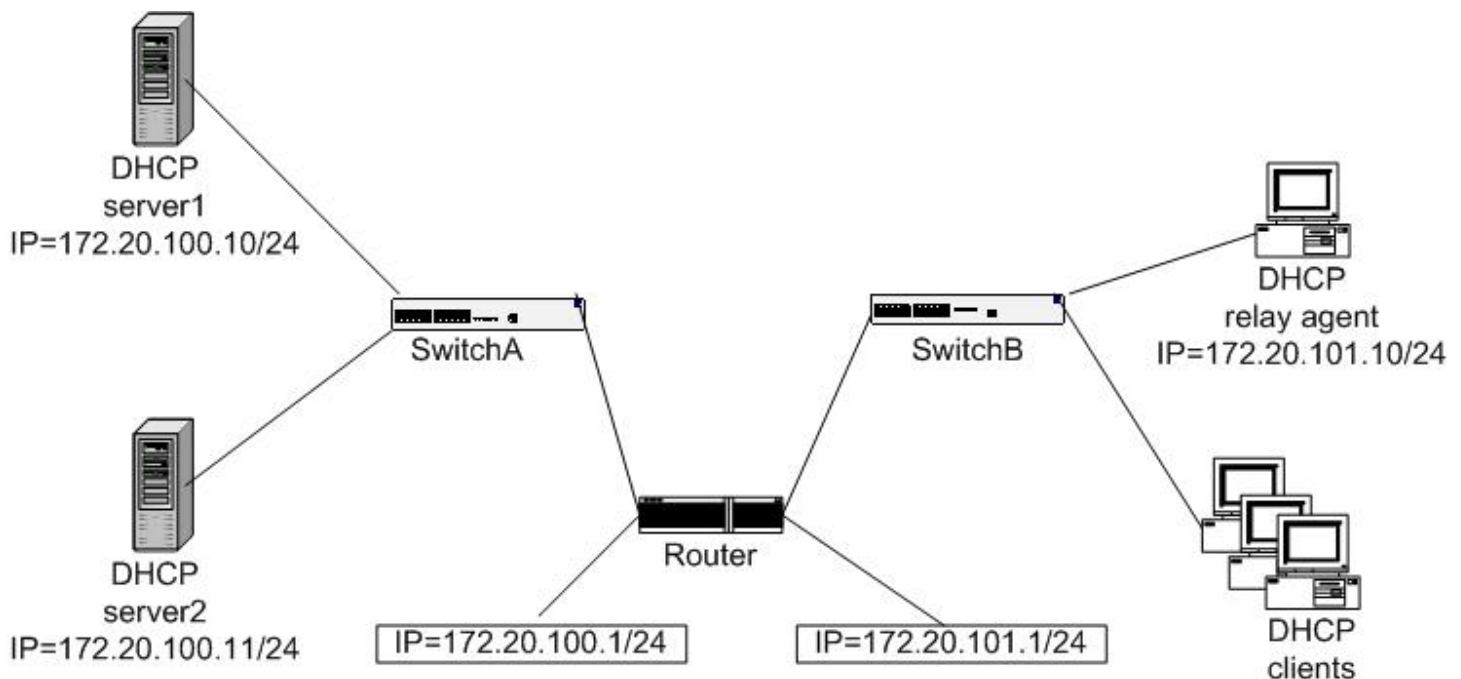
You properly configure your two DHCP servers for redundant DHCP service for all subnets. You configure the DHCP Relay Agent to forward requests to 172.20.101.1.

You discover that all DHCP clients can now communicate with each other, but they cannot communicate with hosts on remote networks. When you run the ipconfig command on one of the DHCP client computers, you receive the information shown in the following table.

IP address	Subnet mask	Default gateway
169.254.0.111	255.255.0.0	None

You must ensure that all DHCP clients can communicate with hosts on remote networks. Which three actions should you perform (Each correct answer presents part of the solution. Choose three.)

A.   Remove 172.20.101.1 from the forwarding list on the DHCP Relay Agent.
B.   Add 172.20.100.1 to the forwarding list on the DHCP Relay Agent.
C.   Add 172.20.100.10 to the forwarding list on the DHCP Relay Agent.
D.   Add 172.20.100.11 to the forwarding list on the DHCP Relay Agent.
E.   Configure the DHCP Relay Agent as a DHCP client.
F.   Change the IP address of the router interface that is connected to SwitchB to 169.254.0.1/16.

Answer: A, C, D
Explanation: The table shows that the client is configured with an APIPA address. The DHCP Relay agent has been configured incorrectly. It should forward requests to a DHCP Server, not to an interface of a router.
A: We must remove the local router interface, 172.20.101.1, from the forwarding list on the DHCP Relay Agent.
C, D: For redundancy we should add both DHCP servers, 172.20.100.10 and 172.20.100.11, to the forwarding list on the DHCP Relay Agent.

Incorrect Answers:
B: We should not add the remote router interface, 172.20.100.1, to the forwarding list on the DHCP Relay Agent. The forwarding list should only include IP addresses of DHCP servers.
E: The DHCP Relay Agent already has a proper IP configuration. There is no need to change the IP configuration of the DHCP Relay agent.

QUESTION NO: 263
You are the administrator of TestKing's network, which links your main office and one branch office. The network consists of a single Active Directory domain in native mode. All servers run Windows 2000 Server and all client computers run Windows 2000 Professional. You use DNS for name resolution. The primary zone server is located at the main office and the secondary zone server is located at the branch office.

Your main office includes a Development department with 200 employees. These users work flexible hours and regularly reconfigure their computers for testing purposes.

Users at the branch office report intermittent problems when they try to access network resources. Sometimes they receive an error message indicating that the network path was not found. Sometimes they are directed to the incorrect server.

You must ensure that all name resolution for branch office users is correct and current. Your solution must involve the fewest possible changes to your existing DNS configuration.

What should you do?

A.   Create a zone and delegate it to the DNS server in the branch office.

B.   Make both servers Active Directory integrated DNS servers.
C.   Configure the primary zone server with a notification list that contains the secondary zone server.
D.   Decrease the retry interval for zone updates on the secondary server.

Answer: C
Explanation: In this scenario we want the DNS server at the branch office to be updated and current. We must ensure that changes to the DNS zone at the main office are immediately transferred to the branch office. We can ensure this behavior by adding the secondary zone server to the notification list on the primary zone server.

Note: Automatic zone transfer occurs during any of the following scenarios:

- When starting the DNS service on the secondary server for a zone
- When the refresh interval time expires for the zone. The default value of the refresh interval is 15 minutes.
- When changes are made to the primary zone and a notify list is configured

Incorrect Answers:
A: The Active Directory only consists of one domain. Creating a new zone is not necessary. We should only use one zone in the domain.

B: Making both DNS Server Active Directory integrated DNS Servers would have many benefits, but it would not be necessary in this scenario since we would like to make as few changes to the current DNS configuration as possible. Furthermore, we also would have to make the DNS zone Active Directory Integrated, not only the DNS servers.

D: Decreasing the retry interval for zone updates, would make the secondary server retry to reload failed zone transfers faster. This could make the secondary DNS zone more current. This is not the best solution, since it would not enforce a zone transfer when a change occurs in the primary zone.

   Note: By default, the retry interval for each zone is set at 10 minutes. The retry interval is used to determine how often other DNS servers that load and host the zone are to retry a request for an update of the zone each time the refresh interval occurs.

QUESTION NO: 264
You are the administrator of TestKing's network. Your network consists of a single segment, which you divide into four segments by installing routers. The relevant portion of the new network configuration is shown in the exhibit.
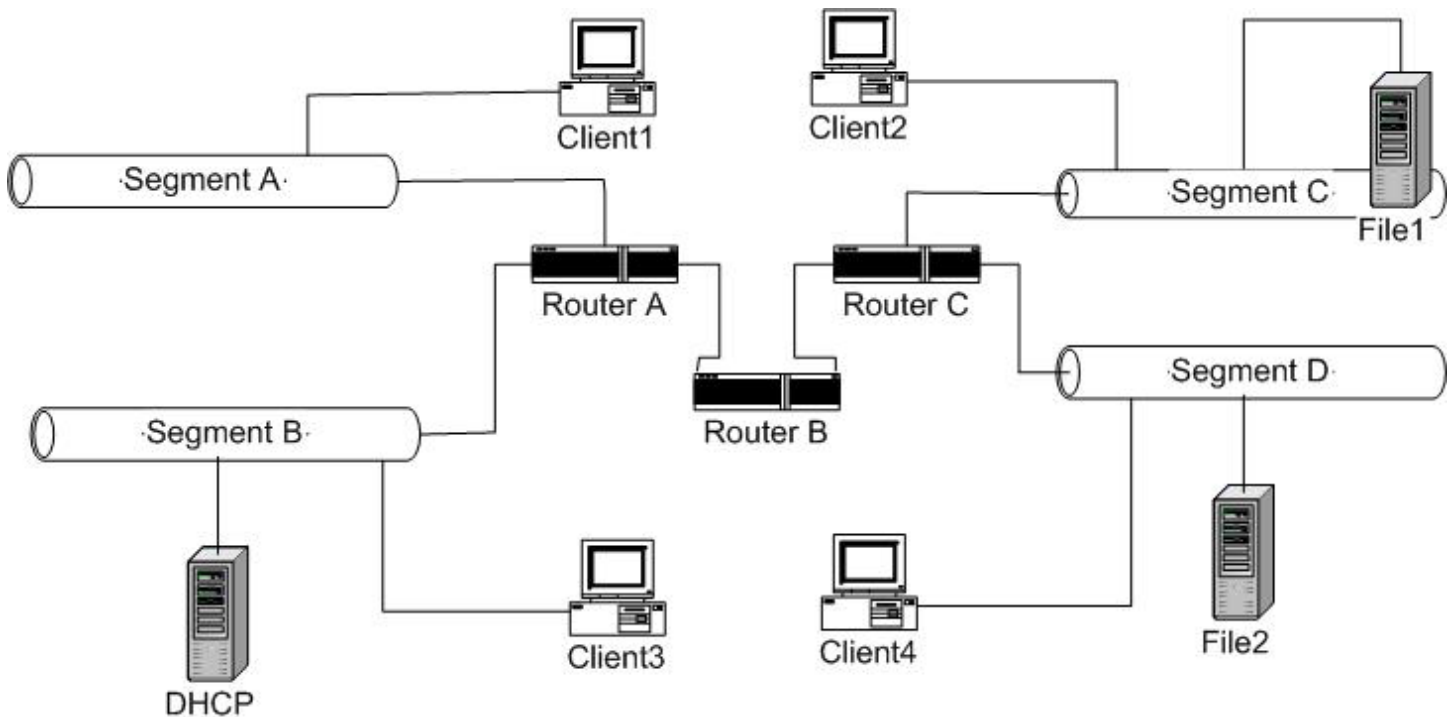
The new configuration includes a DHCP server running Windows 2000 on Segment B. Each new segment also includes one client computer running Windows 2000 Professional. These computers are named Client1 through Client4.

Segment C and Segment D each include one file server running Windows 2000 Server. The file servers are named File1 and File2.

You configure the client computers as DHCP clients. You assign static IP addresses to the Windows 2000 Server computers. You create four scopes on the DHCP server with the correct IP addresses.

When you test your configuration, you discover that Client1, Client2, and Client4 cannot communicate with any other computers on the network. Client3 can communicate with File1 and File2, but not with other client computers.

You need to ensure that all client computers can communicate with both file servers and with each other. Which action or actions should you perform?

- A. Configure Client1, Client2, and Client4 as DHCP Relay Agents.
- B. Configure Client1, Client4, and File1 as DHCP Relay Agents.
- C. Configure Router A to forward BOOTP packets, and configure File1 and File2 as DHCP Relay Agents.
- D. Configure Router B to forward BOOTP packets, and configure File1 and File2 as DHCP Relay agents.

Answer: C
Explanation: In this scenario apparently the DHCP configuration information is not able to reach the remote subnets. The most likely cause is that the routers are not BOOTP-enabled and therefore block DHCP traffic. We must ensure that Client1, Client2, and Client4 can communicate with other computers on the network. We already know that File1 and File2 are able to communicate with other computers, in particular with Client3. We could therefore use them as DHCP Relay agents. This will ensure that Client2 and Client4 receive proper IP configuration. We must also ensure that Client1 can work as a DHCP client. We ensure this by configuring RouterA to forward BOOTP packets.

Note: Only Windows 2000 Server computers, not Windows 2000 Professional computers, can be configured as DHCP Relay Agents.

Incorrect Answers:
A: Client1, Client2 and Client4 are not able to function as DHCP Relay agents since they run Windows 2000 Professional.
B: Client1 and Client4 are not able to function as DHCP Relay agents since they run Windows 2000 Professional.
D: By examining the exhibit, we see that in order for Client1 to receive IP configuration from the DHCP Server RouterA, not RouterB, must be BOOTP enabled.

QUESTION NO: 265
You are the administrator of TestKing's network. You are configuring your users' portable computers to allow users to connect to company network by using Routing and Remote Access. You test the portable computers on the LAN and verify that they can successfully connect to resources on the company network by name. When you test the connection through Remote Access, all of the portable computers can successfully connect, but they cannot access files on computers on different segments by using the computer name.

What should you do to resolve this problem?

   A.   Set the authentication method to **Allow remote systems to connect without authentication.**
   B.   Enable the computer account for each portable computer.
   C.   Change the computer name on each portable computer.
   D.   Install the DHCP Relay Agent on the Remote Access server.

Answer: D
Explanation: The portable computers are able to gain remote access, but they cannot access files on computers on different segments by using computer names. Apparently they have not be received the proper IP configuration, default gateway and DNS server for example, from a DHCP server; instead they receive IP configuration from the RRAS server. By installing and configuring a DHCP Relay Agent on RRAS server the

portable computers would receive proper IP configuration and would be able to access resources on different remote segments by name.

Incorrect Answers:

A: This is not an authentication problem. The laptops gain remote access, but they have problems accessing resources. Allowing the portable computers to gain remote access without authentication would not solve the problem, and at the same time it would introduce a security risk.

B: This is not an authentication problem. The laptops gain remote access, but they have problems accessing resources. The computer accounts for the remote computers are already enabled since these computers were able to connect to resources when they were connected to the LAN.

C: Since the portable computers were able to connect to resources when they were connected to the LAN, there is no need to change their computer names.

QUESTION NO: 266
You are the administrator of TestKing's network. All servers run Windows 2000 Server and all client computers run Windows 2000 Professional. All client computers are DHCP clients, and all servers have static IP addresses. You use both WINS and DNS for name resolution.

For redundancy, the network includes two WINS servers, Corp1 and Res1. Both are configured to use the automatic partner configuration. Corp1 is managed by the Information Technology department and Res1 is managed by the Research department. The network administrators in the Research department use static entries in the WINS database of Res1 to manage their servers.

Users report that they can no longer access several servers in the Research department that were previously accessible. You conclude that WINS is incorrectly resolving the server names. When you analyze the WINS database, you discover that it contains incorrect records of the mappings for these servers. All other WINS records are correct and unaffected.

You need to ensure that the correct records appear on each WINS server. You must accomplish this goal with the least possible disruption of workflow.

What should you do?

    A.   Delete the WINS database from Corp1 and restore it from the most recent backup.
    B.   Delete the WINS database from Res1 and restore it from the most recent backup.
    C.   On Corp1, correct the WINS entries and increase the version number for the records of the research department servers.
    D.   On Res1, correct the WINS entries and increase the version number for the records of the research department servers.
    E.   Perform a database consistency check on Corp1.
    F.   Perform a database consistency check on Res1.

Leading the way in IT testing and certification tools, www.testking.com

Answer: D

Explanation: Res1 contains static records. Static records are added manually by the Administrator. Apparently some of the manually added records are incorrect. By correcting these records and increasing the version number for these records, the records would be replicated to Corp1, and the old incorrect records on Corp1 would be replaced as well.

Incorrect Answers:

A: We need to replace the records on Res1 not on Corp1 since Res1 contains static records.

B: The most recent backup would have lower, not higher, version numbers than records on Corp1. The records would not replace the records on Corp1.

C: We need to replace the records on Res1 not on Corp1 since Res1 contains static records.

E: Fixing the records on Corp1 would not help since Res1 has static records.

F: A database consistency check would not fix the static records on Res1.

QUESTION NO: 267

You are the network administrator for your company. You plan to create a fully routed network. You configure three Windows 2000 Server computers as routers, as shown in the following diagram.
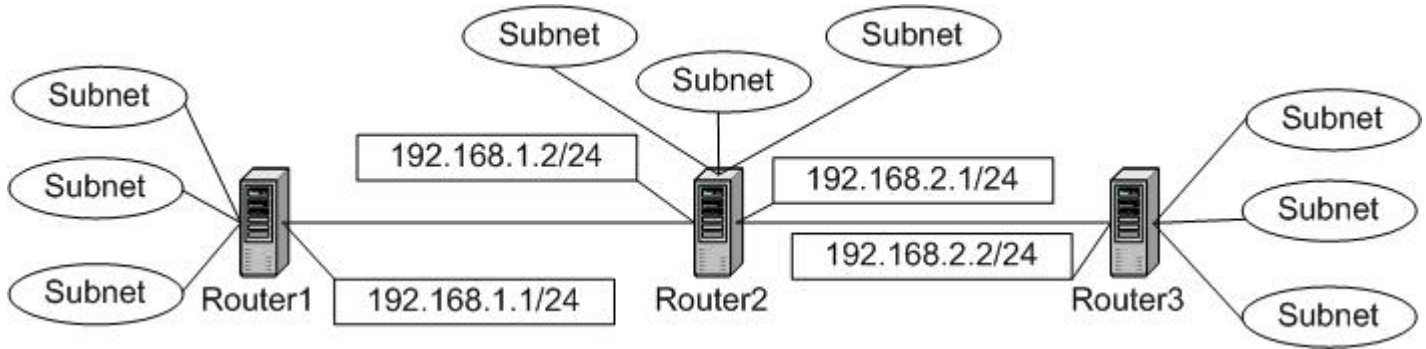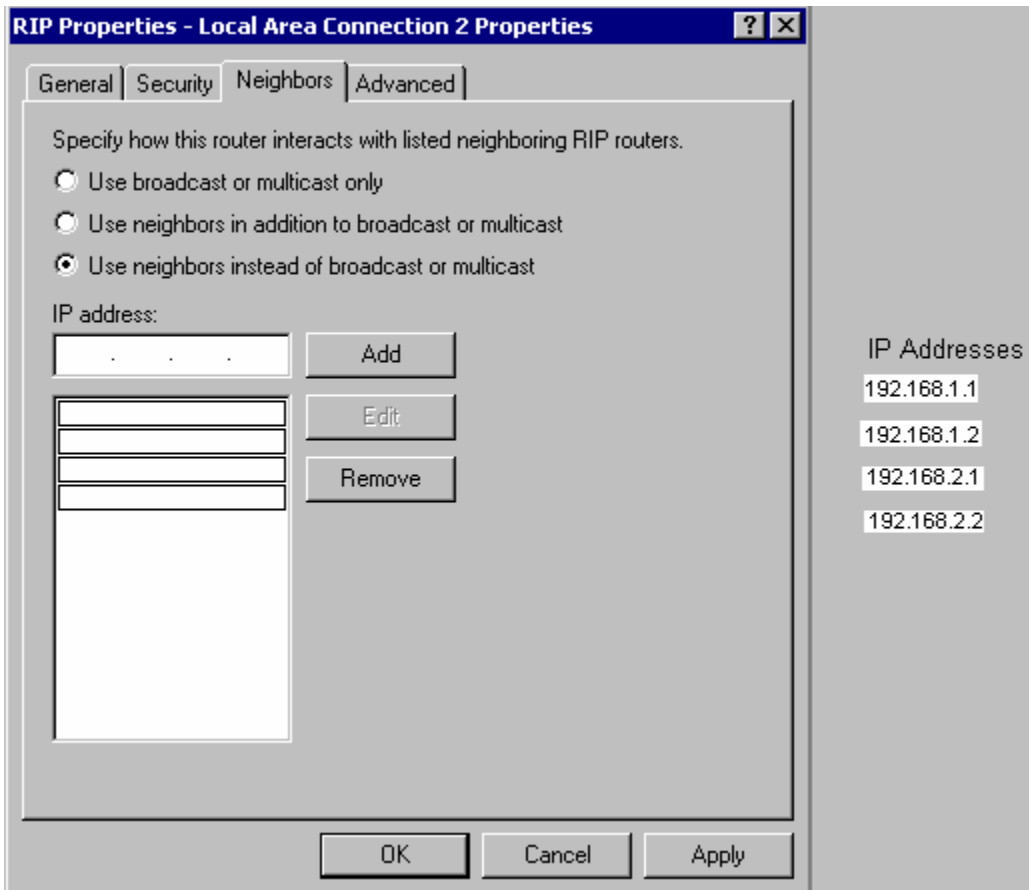

You install RIP on all three routers, accepting all default settings. To ensure that RIP traffic is received only by the RIP routers, you configure the RIP properties on all three routers to use neighbors instead of broadcast or multicast routing.
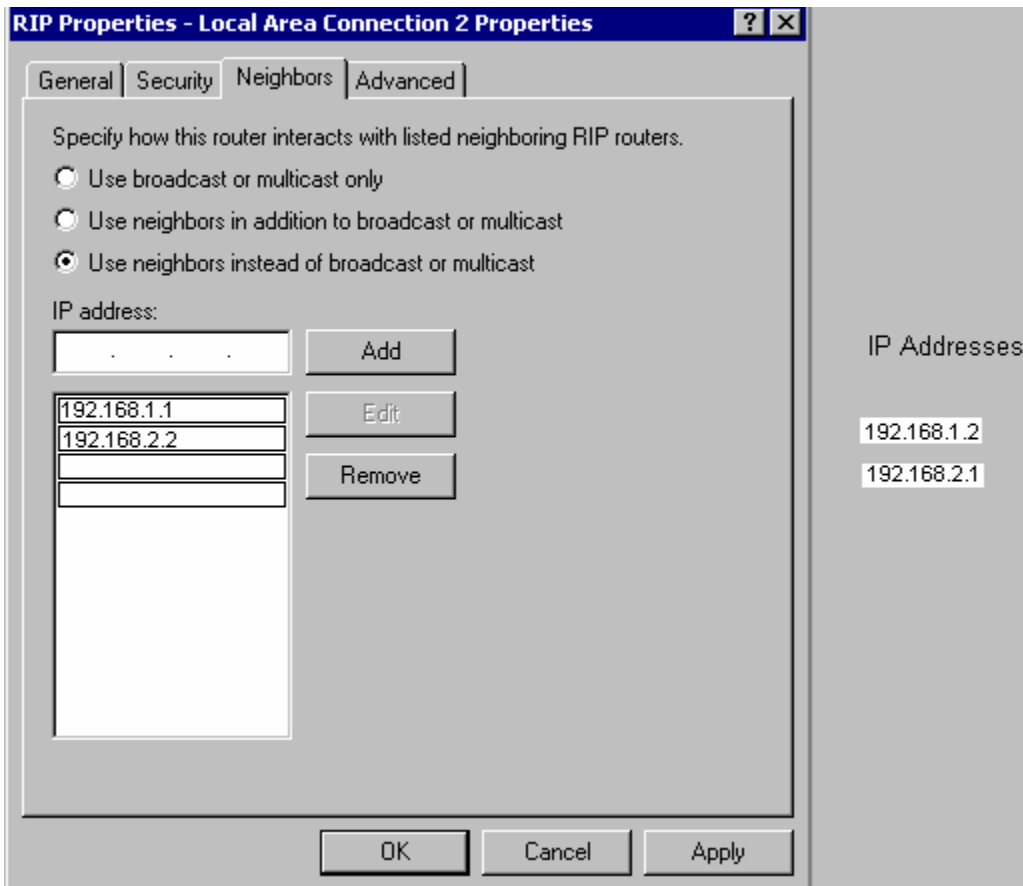
You now discover that hosts on Router1 subnets can communicate only with hosts on other Router1 subnets. To correct this problem, you need to reconfigure the RIP properties on the 192.168.1.2 interface on Router2.

What should you do?

To answer, drag the correct IP address or addresses to the appropriate locations in the dialog box. Use the minimum number of necessary IP addresses.

RIP Properties - Local Area Connection 2 Properties

General | Security | Neighbors | Advanced

Specify how this router interacts with listed neighboring RIP routers.

○ Use broadcast or multicast only

○ Use neighbors in addition to broadcast or multicast

● Use neighbors instead of broadcast or multicast

IP address:

[. . .]   Add

Edit

Remove

IP Addresses

192.168.1.1

192.168.1.2

192.168.2.1

192.168.2.2

OK   Cancel   Apply

Answer:

Explanation: We must manually configure the neighbors of the 192.168.1.2 interface on Router2. We must add the appropriate interface of Router1 and Router3. These are 192.168.1.1 and 192.168.2.2 respectively.

Incorrect answers:

192.168.1.2: 192.168.1.2 is the interface itself. It should not be added as a route.

192.168.2.1: 192.168.2.1 is another interface on Router2 and should not be added.

QUESTION NO: 268
You are the network administrator for your company, which uses a single network address of 172.16.48.0/24. All computers on the network run Windows 2000. The network includes 12 resource servers and 200 client computers, all configured as DHCP clients. The network also includes dynamic DNS servers.

Your network contains one Windows 2000 DHCP server with a manually assigned IP address 172.16.48.254. This server uses all default settings. While you are performing hardware BIOS upgrades on this server, you inadvertently erase the storage containing the DHCP database. You have no recent backup.

You need to reconfigure the DHCP server. Your solution must involve the least possible disruption to network users.

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

A. Set the **Conflict Detection Attempts** setting to 1.
B. Add an exclusion range for the 12 resource servers.
C. Create a scope with a range of 172.16.48.1 to 172.16.48.220.
D. Create a scope with a range of 172.16.48.21 to 172.16.48.254.
E. Run the **ipconfig /registerdns** command on each server and each client computer on the network.
F. Run the **ipconfig /flushdns** command on each server and each client computer on the network.

Answer: A, C
Explanation:
A: By setting the Conflict Detection Attempts on the DHCP server to 1, (the default value is 0), the DHCP server pings the lease IP address one time to detect any conflicts, before actually leasing the IP address.

C We should configure the DHCP server with an appropriate scope which does not include the DHCP server itself.

Note: The DNS records will automatically be updated when the computers try to lease a new IP address.

Incorrect Answers:
B: The servers have dynamic IP addresses. Only computers with static IP addresses should be excluded from the range.

D: We should not include the IP address of the DHCP server itself, 172.16.48.254, in the DHCP scope (unless we make an exclusion).

E, F: The DNS records will automatically be updated when the computers try to lease a new IP address. There is no need to manually register each client computer.

QUESTION NO: 269
You are the network administrator for Wingtip Toys, which is the parent company of Tailspin Toys. Wingtip Toys's main office is located in Philadelphia. The Tailspin Toys branch office is located in New York City. Your network consists of two Windows 2000 domains named wingtiptoys.com and tailspintoys.com. The network is configured as shown in the exhibit.
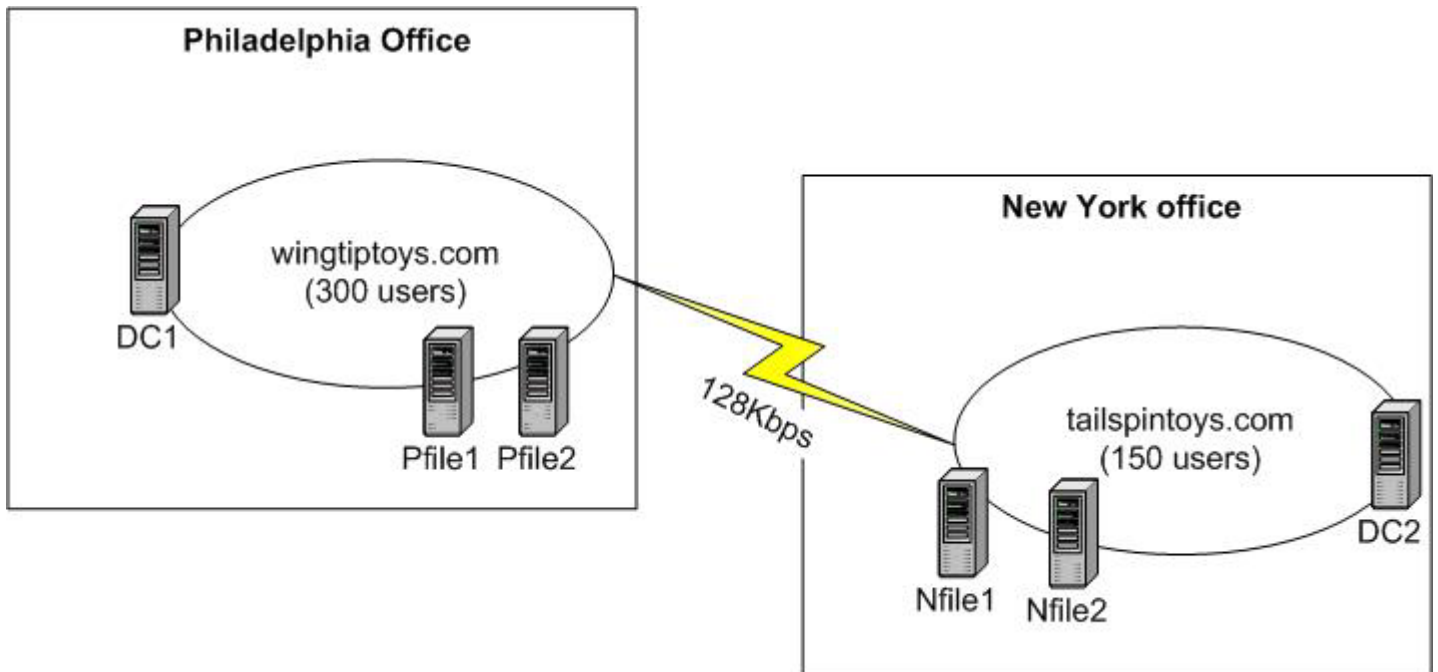
Each office includes a single domain controller running Windows 2000 Server. These computers are named DC1 and DC2. Each one runs the DNS Server service and an Active Directory integrated zone.

Each office also includes two file servers running Windows 2000 Server. These computers are named Pfile1, Pfile2, Nfile1, and Nfile2. Users at the Philadelphia office occasionally access files on Nfile1 and Nfile2, and users at the New York office occasionally access files on Pfile1 and Pfile2.

Users at both offices report that they often receive an error message when they try to access files from the other office. The error message states: "Network path could not be found."

You need to correct this problem. Your solution must involve the fewest possible changes to the configuration of DC1 and DC2.

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

    A.   Install the DNS Server service on Pfile1 and create a secondary zone for wingtiptoys.com. Install the DNS Server service on Nfile1 and create a secondary zone for tailspintoys.com.
    B.   Install the DNS Server service on Nfile1 and create a secondary zone for wingtiptoys.com. Install the DNS Server service on Pfile1 and create a secondary zone for tailspintoys.com.
    C.   Configure the New York domain controller to forward DNS requests to Nfile1 first. Configure the Philadelphia domain controller to forward DNS requests to Pfile1 first.
    D.   Configure the New York domain controller to forward DNS requests to Pfile1 first. Configure the Philadelphia domain controller to forward DNS requests to Nfile1 first.
    E.   Promote Nfile1 to a domain controller. On Nfile1, install the DNS Server service and create an Active Directory integrated zone.

F.   Promote Pfile1 to a domain controller. On Pfile1, install the DNS Server service and create an Active Directory integrated zone.

Answer: B, C
Explanation: We should implement a DNS solution where the clients use a local DNS server for remote name resolution. This will improve performance, since the offices are connected by a slow WAN link.

B: We should install one new DNS server in each location. We want to make minimal changes to the domain controllers so we should not install the DNS servers in the domain controllers; instead we use Pfile1 and Nfile1. We create secondary zones for the remote domain on these DNS servers: we make a secondary zone for tailspintoys.com on Pfile and a secondary zone for wingtiptoys.com on Nfile1.
C: We should configure DC1 to forward its requests to the local DNS server Pfile1, and DC2 should be configured to use the local DNS server Nfile1.

Incorrect Answers:
A: Creating a secondary zone for the local zone would give redundancy, but it would not improve name resolution performance. Name resolution traffic would still have to travel over the slow WAN connection.
D: The DNS Servers DC1 and DC2 should forward DNS requests to the local DNS server, not the remote DNS server.
E, F: Another Active Directory integrated zone in each location would provide redundancy, but it would not improve name resolution performance. Name resolution traffic would still have to travel over the slow WAN connection.

QUESTION NO: 270
You are the network administrator for your company. Your network includes 100 Windows 2000 Server computers, 5,000 desktop computers running Windows 2000 Professional, and 1,000 portable computers running Windows 98.

Twenty servers are either domain controllers or DHCP servers. The remaining servers are Web servers and database servers that host multiple Web sites. Each Web site has a unique IP address.

All servers need specific IP addresses, but none of the client computers do. You plan to use DHCP to assign as many network configuration settings as possible to the computers on the network. On your DHCP servers, you create scopes that include all possible IP addresses that can be used in your company.

Which additional parameters must you configure on the DHCP scopes to support the various hosts?

To answer drag the correct configuration to the appropriate computer type. You might need to use some configurations more than once. Use the minimum number of necessary configurations.

DHCP servers	Drag item here

Domain controllers	Drag item here

Web servers	Drag item here

IP address reservation

IP address exclusion

Answer:

| DHCP servers | IP address exclusion |

| IP address reservation |

| Domain controllers | IP address reservation |

| IP address exclusion |

| Web servers | IP address reservation |
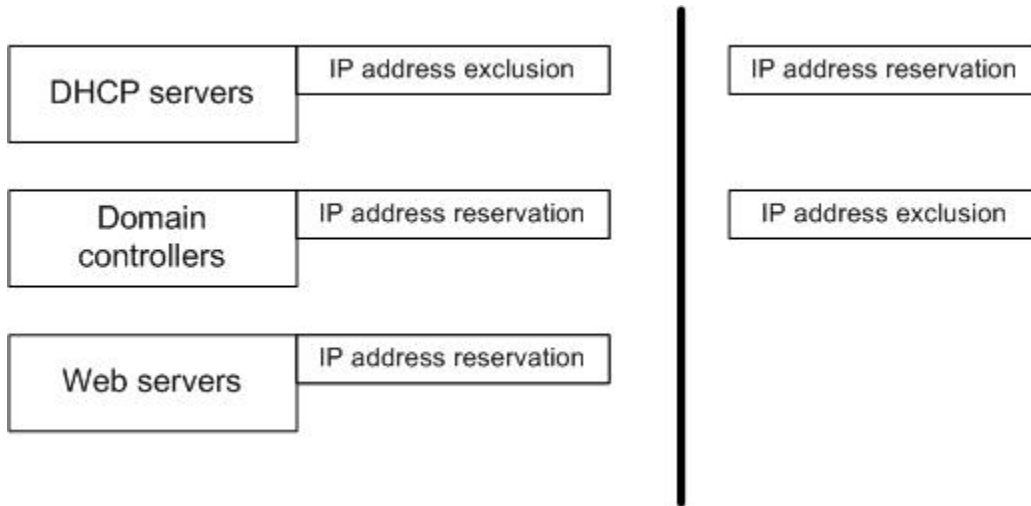
Explanation:

The IP address of the DHCP server must be excluded from the range.

Each Web server should use the same IP address. To minimize IP configuration we should make IP address reservations for the Web servers.

Domain controllers should use static IP addresses as a best practice. We should use reservations, instead of exclusions, to maximize the use of DHCP.

QUESTION NO: 271

You are the administrator of TestKing's network, which consists of a single segment and a single Windows 2000 domain. In the near future, your company plans to make several changes to your DNS, WINS, and routing environments.

Currently, you use the network address 172.25.10.0/24 for 200 client computers and three Windows 2000 domain controllers. All client computers are DHCP clients. Your DHCP server is configured with a single scope that has the characteristics shown in the following table.

DHCP scope	IP address range	IP address reservations	IP address exclusions
172.25.10.0/24	175.25.10.6 to 172.25.10.254	None	None

You want to assign specific IP addresses to your three domain controllers. You select 172.25.10.10, 172.25.10.11, and 172.25.10.12 as the IP addresses. However, when you review the list of active leases, you notice that all three IP addresses are leased out to client computers for a duration of eight days.

You need to assign the IP addresses to the domain controllers in a way that will minimize future administrative effort.

What should you do?

A.   Delete the active leases for the three IP addresses.
      Create individual IP address reservations that allow each domain controller to use one of the three IP addresses.
      Configure the domain controllers as DHCP clients.

B.   Create individual IP address reservations that allow each domain controller to use one of the three IP addresses.
      Run the **ipconfig /renew** command on each client computer that has an active lease for one of the three IP addresses.
      Configure the domain controllers as DHCP clients.

C.   Delete the active leases for the three IP addresses.
      Create an exclusion range that consists of three IP addresses.

D.   Create an exclusion range that consists of the three IP addresses.
      Run the **ipconfig /renew** command on each client computer that has an active lease for one of the three IP addresses.

Answer: B
Explanation: First we should make IP reservations for the domain controllers. Then we should force a renewal of the IP configuration on the clients with the active lease for these IP addresses. This will force the clients to get new IP addresses since their old addresses are now reserved. Finally we configure the Domain Controllers as DHCP clients.

Incorrect Answers:
A: Deleting the leases would not immediately remove the IP configuration from the clients that have the IP configuration intended for the domain controllers. Not until they either are restarted or they try to renew the lease will the client computers get new IP configuration.

C: Deleting the leases would not immediately remove the IP configuration from the clients that have the IP configuration intended for the domain controllers. Not until they either are restarted or they try to renew the lease will the client computers get new IP configuration.

The Domain controllers should be configured as DHCP clients.

D: The Domain controllers should be configured as DHCP clients.

QUESTION NO: 272
You are the administrator of TestKing's network, which consists of two segments that are connected by a router. The network contains two DHCP servers. The relevant portion of its configuration is shown in the exhibit.
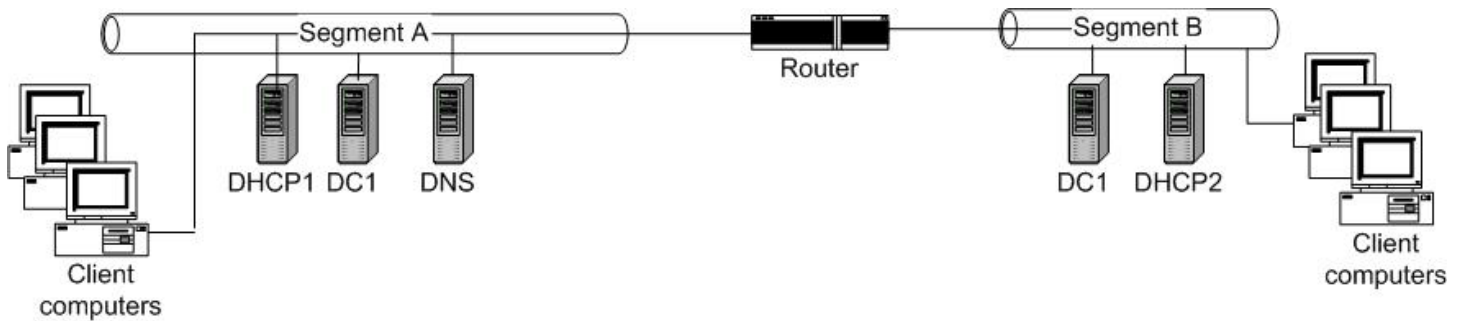
The network includes two domain controllers named DC1 and DC2. The network also includes 50 client computers on each segment. The domain controllers have static IP addresses and the client computers are DHCP clients.

You configure the DHCP servers with the characteristics shown in the following table.

DCHP server	DCHP scope	IP address range	IP address reservation	IP address exclusions
DHCP1	172.25.10.0/24	172.25.10.6 to 172.25.10.254	None	None
DCHP2	172.25.11.0/24	172.25.11.6 to 172.25.11.254	None	None

You decide to configure the domain controllers to use DHCP to obtain IP addresses. You create a reservation for both domain controllers on DHCP1. You use IP address 172.25.10.4 for DC1 and 172.25.11.5 for DC2. You create static A (host) records in your DNS server for the two domain controllers.

When you restart the domain controllers, you discover that client computers can communicate only with DC1.

You need to ensure that client computers can communicate with both domain controllers. What should you do?

    A.   Create a reservation on DHCP2 that assigns 172.25.11.5 DC2.
    B.   Create a reservation on DHCP1 that assigns 172.25.11.5 DC2.
    C.   Modify the server options on DHCP2 to include the IP address of your DNS server.
    D.   Modify the server options on DHCP1 to include the IP address of your DNS server.

Answer: A
Explanation: The IP address of DC2, 172.25.11.5, is not within the DHCP scope, 172.25.10.0/24, of DHCP1. The reservation must be made on DHCP2 on which the DHCP scope is 172.25.11.0/24.
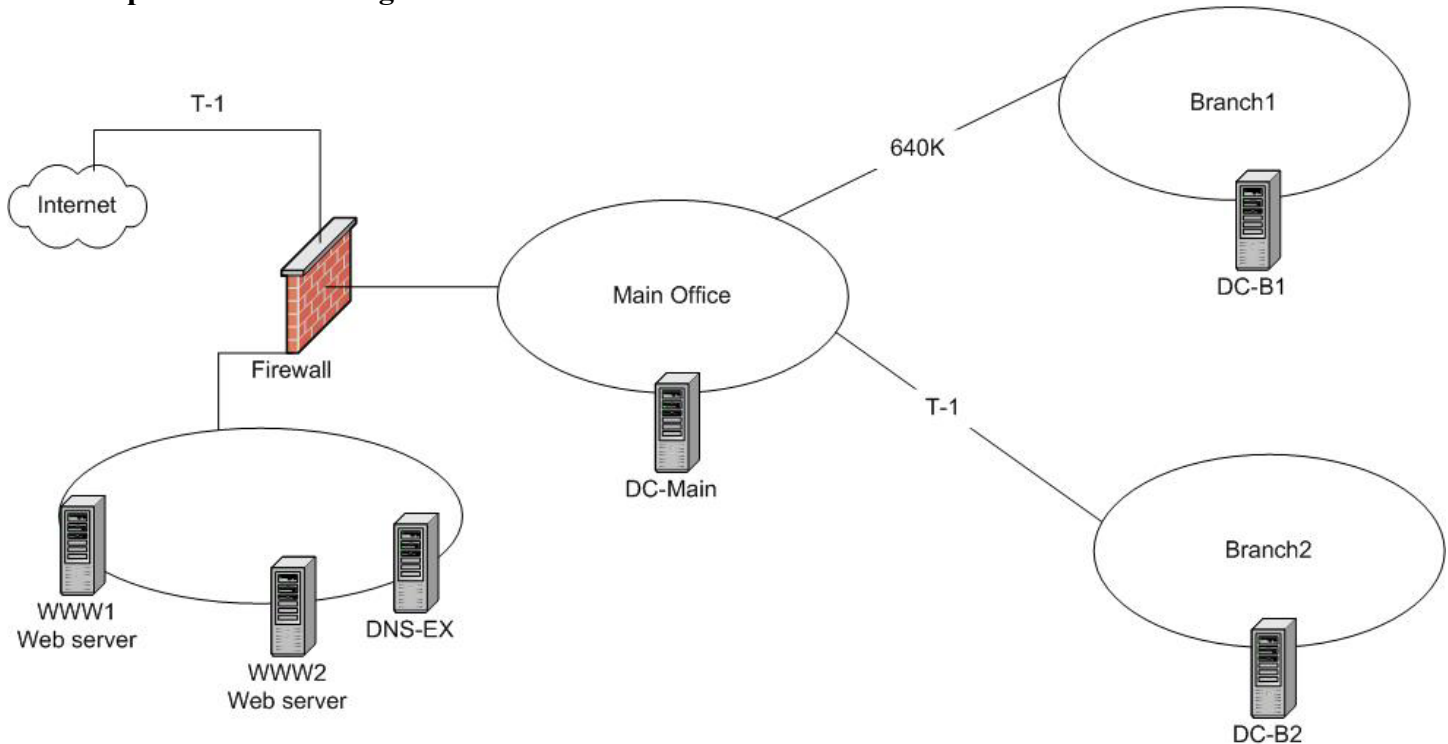
Incorrect Answers:
B: We already have a reservation for DC2 on DHCP1.
C, D: DC1 is working correctly, so there is no need to reconfigure the DNS setting on the DHCP servers.

QUESTION NO: 273
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The relevant portion of its configuration is shown in the exhibit.

The main office contains 2,000 client computers. Branch1 contains 350 client computers. Branch2 contains 600 client computers. Each office has its own domain controller. The domain controllers are named DC-main, DC-B1, and DC-B2.

You DMZ network includes two Web servers that run Windows 2000 Server and Internet Information Services (IIS). Each web server contains a copy of a Web application used by internal users. Each Web server also hosts the company Web site, which is available to external users through the Internet. Company policies require that internal network information must never be accessible to external users.

You install the DNS Server service on the domain controllers in each office and on a stand-alone Windows 2000 Server computer in the DMZ network.

Now you need to ensure that all company users can access the Web application, and that external users can access the company Web site. You also need to ensure that all access is evenly distributed across the

two Web servers. Your solution must reduce name resolution traffic, and zone transfer traffic across the WAN links, and it must provide redundancy if any DNS server fails.

What should you do?

To answer, drag the appropriate DNS zone type and configuration option to each DNS server. You might need to use some zone types and configuration options more than once.

	DC-Main	DC-B1 & DC-B2	DNS-EXT
Zone type:			
Record type:	A (host) records for Web servers	A (host) records for Web servers	A (host) records for Web servers
Configuration option:			

Possible zone types:	Active Directory Integrated zone	Standard primary zone	Standard secondary zone
Possible configuration options:	Enable recursive queries.	Enable dynamic updates.	Enable round robin.

Answer:

	DC-Main	DC-B1 & DC-B2	DNS-EXT
Zone type:	Active Directory Integrated zone	Active Directory Integrated zone	Standard primary zone
Record type:	A (host) records for Web servers	A (host) records for Web servers	A (host) records for Web servers
Configuration option:	Enable round robin.	Enable round robin.	Enable round robin.
Possible zone types:	Active Directory Integrated zone	Standard primary zone	Standard secondary zone
Possible configuration options:	Enable recursive queries.	Enable dynamic updates.	Enable round robin.

Explanation: The proposed solution meets the following requirements:
- all company users can access the Web site.
  We have set up DC-Main, DC-B1 & DC-B2 correctly.
- all access is evenly distributed across the Web servers.
  We have enabled Round Robin on all DNS servers.
- reduce the name resolution and zone traffic across the WAN links.
  This is assured since we are use Active Directory Integrated zones on the domain controllers.
- provides redundancy if any DNS server fails.
  This is met on the domain controllers, but not on DNS-ext. If DNS-ext fails then there is no redundancy for the external users' access to the company Web site.
  This suggests that we should use a secondary zone on DNS-ext. DNS-ext cannot, however, be allowed to access any internal resources so this is out of the question.

QUESTION NO: 274
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain. The network includes 15 computers running Windows 2000 Server and 150 computers running Windows 2000 Professional. The network is divided into two subnets, with all servers on one subnet and all client computers on the other. Two of the servers, AX1 and AX2, have DNS and DHCP installed and configured. All client computers use DHCP for IP addressing, and all servers have static IP addresses.

You assign the default Secure Server IPSec policy to all servers. However, users report that they can no longer log on to the domain.

You must ensure that server data remains encrypted, and that all users can log on to the domain. What should you do?

    A.   Increase the time skew for Kerberos authentication to eight minutes.
    B.   Configure a custom IPSec policy to respond securely to the server subnet for all client computers.
    C.   Configure all servers with the Server (Request Security) IPSec policy.
    D.   Install an enterprise certificate server on AX1 and issue certificates to all client computers.

Answer: B
Explanation: We have configured the servers to require IPSec by assigning the Secure Server IPSec policy to all servers. The clients, however, have not been configured for IPSec. Now the clients are unable to communicate with the server, in particular they are unable to log on to the domain. Be configuring the clients to respond securely (with encryption), they would be able to communicate with servers using encryption.

Incorrect Answers:
A: We must configure the clients for encryption. Time skew does not apply here.

C: If we change the IPSec policy on the servers from require security to request security, the clients and the servers would be able to communicate. However, the traffic would be unencrypted since the clients have not been configured for IPSec.

D: There is no need to install a certificate server.

QUESTION NO: 275
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain named testking.com.

The network is configured as a single segment with one DHCP server. The segment uses the network address 172.30.10.0/24 for 200 client computers and three Windows 2000 domain controllers. All client computers are DHCP clients.

The DHCP server is configured with a single scope, which has the characteristics shown in the following table.

DHCP scope	IP address range	IP address reservation	IP address exclusions
172.30.10.0/24	172.30.10.10 to 172.30.10.254	None	None

Your three domain controllers must always receive the IP addresses 172.30.10.10, 172.30.10.11, and 172.30.10.12. However, when you review the list of active leases, you discover that all three of these IP addresses are leased out to client computers for a duration of eight days.

You need to ensure that these IP addresses will be assigned to the domain controllers. You must minimize any disruption of network connectivity for the three client computers that currently use these addresses.

What should you do?

To answer, click the Select and Place button, and then drag the appropriate actions to the right column in the correct order. Use each possible action only once. Use the minimum number of necessary actions.

Possible actions - select from these

Restart the client computers

Create an additional scope on the DHCP server

Run the ipconfig/renew command on the client computers

Add IP address reservations for the domain controllers.

Change the DHCP scope to begin at 172.30.10.14

Add an exclusion to the DHCP scope.

Necessary actions - place here

Place first action here

Place second action here

Place third action here

Answer:

Possible actions - select from these | Necessary actions - place here

Restart the client computers

Create an additional scope on the DHCP server

Change the DHCP scope to begin at 172.30.10.14

Add an exclusion to the DHCP scope.

Add IP address reservations for the domain controllers.

Run the ipconfig/renew command on the client computers

Place third action here

Explanation:
Step 1: We must reserve these specific IP address for the domain controllers.
Step 2: We must free these IP address as they are already in use. We renew the IP lease on the client computers. As their current IP addresses are now reserved they will receive new IP addresses.
Step 3: No further action is required. The only action required would be to use the **ipconfig /renew** command on the servers or to start/restart them. These actions are not listed however.

Incorrect Answers:
Restart the client computers

We just need to renew the IP configuration of the DHCP clients. We don't have to restart to achieve this goal.

Create an additional scope on the DHCP server, Change the DHCP scope to begin at 172.30.10.14

There is no need to create an additional scope. On the contrary, this would be bad idea.

Add an exclusion to the DHCP scope.

If some hosts used static IP address we could consider using exclusions. However, since the servers are DHCP clients we should not use exclusions. The servers would be unable to receive their appropriate IP addresses through DHCP if the addresses were excluded.

QUESTION NO: 276

You are the network administrator for you company, which includes a main office in Tokyo and one branch office in Durban. Each office has a persistent connection to the Internet, but no direct connection exists between the two offices.

Both offices maintain firewalls that allow only outbound Web and virtual private network (VPN) traffic to the Internet. In front of the firewall in Tokyo, a router is connected to two different Internet service providers (ISPs). Also in Tokyo, an L2TP server is connected to the Internet and to the local network. The Durban office is connected to the Internet by a single ISP connection.

Computers in Durban occasionally need to communicate with servers in Tokyo. The Durban office includes a Windows 2000 Server computer named TestKing3.

You need to configure TestKing3 to provide routing from the Durban office to Tokyo. What should you do?

A. Configure TestKing3 as a demand-dial router to connect to the L2TP server in Tokyo.
B. Configure TestKing3 as a demand-fail router to connect to the router in front of the firewall in Tokyo.
C. Configure TestKing3 as an OSPF router in the Internet.
D. Configure TestKing3 as a RIP router on the Internet.
E. On TestKing3, enable IP forwarding and configure static routes to Tokyo.

Answer: A
Explanation: The L2TP server in Sydney is the only point of entry since the firewall does not allow any inbound traffic. We must therefore configure a VPN connection from TestKing3 in Durban to the L2TP server in Sydney.

Incorrect Answers
B: There is no such thing as a demand-fail router.
C, D: We want to enable routing between the two LANs. We should not configure the computer as an Internet Router.
E: The only point of entry in Sydney is the L2TP server. We must create a VPN connection to it. We can't just use static routes to Tokyo.

QUESTION NO: 277
You are the administrator for TestKing's network. The relevant portion of your network configuration is shown in the following diagram.
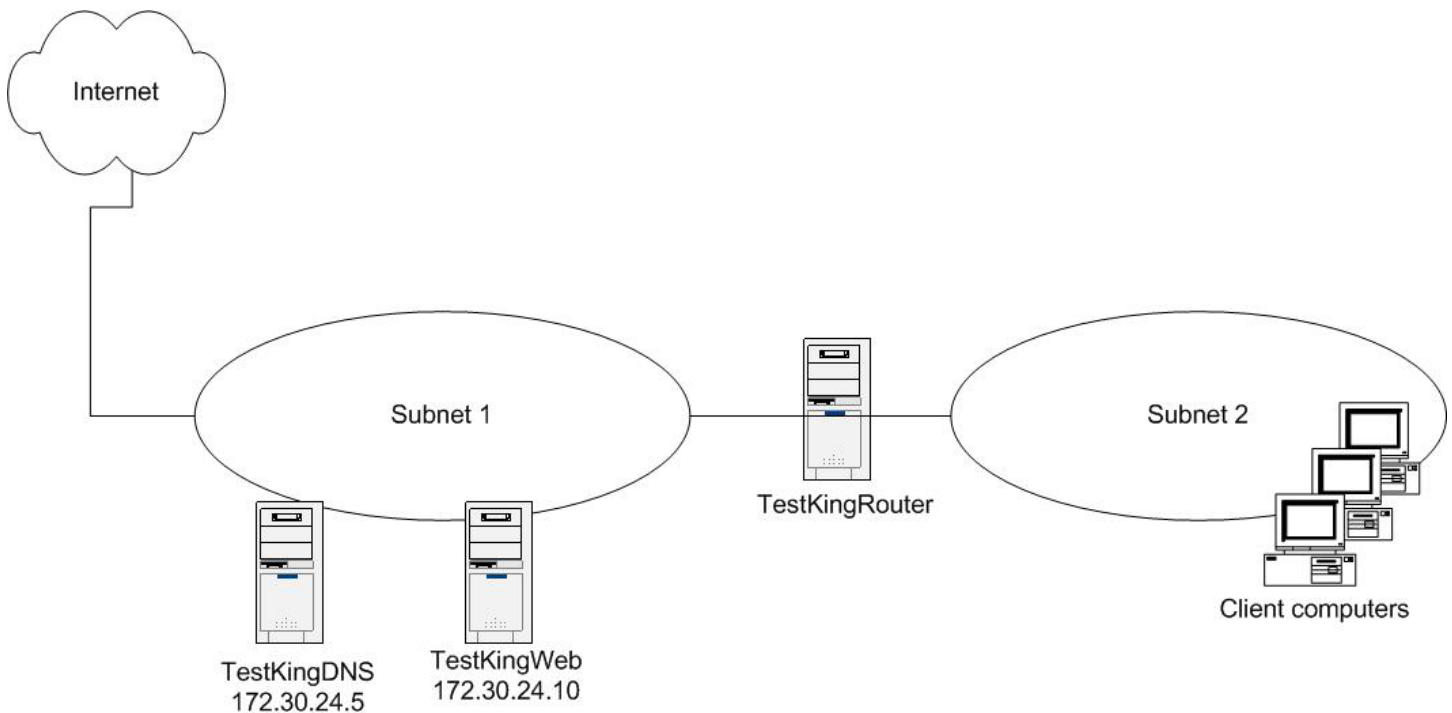
All client computers run Windows 2000 Professional. TestKingDNS runs Windows 2000 Server and the DNS Server Service. TestKingWeb runs Windows 2000 Server and Internet Information Services (IIS). TestKingRouter runs Windows 2000 Server and Routing and Remote Access.

On TestKingRouter, the network adapter for Subnet2 is configured for packet filtering as shown in the exhibit.
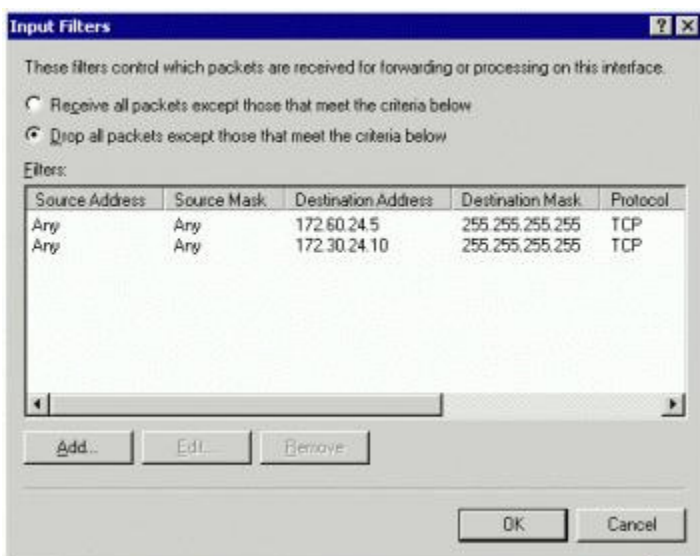
Users on Subnet 2 must be able to use TestKingDNS for name resolution. They must also access a Web application on TestKingWeb. No other traffic must be allowed to pass from Subnet 2 to Subnet 1.

TestKingDNS and TestKingWeb must be able to access files on TestKingRouter. No other traffic must be allowed to pass from Subnet 1 to Subnet 2.

Currently, users can access TestKingDNS and TestKingWeb. However, you discover that file sharing traffic from TestKingWeb and TestKingDNS is being transmitted on Subnet 2.

Which action should you perform on TestKingRouter to correct the problem?

   A.   Create an input filter in the network adapter for Subnet1. Configure the filter to receive only traffic that is responding to an existing session or is directed to TestKingRouter.
   B.   Create an output filter on the network adapter for Subnet1. Configure the filter to receive only traffic that is responding to an existing session or is directed to TestKingRouter.
   C.   Create an output filter on the network adapter for Subnet2. Configure the filter to receive only traffic that is responding to an existing session or is directed to TestKingRouter.
   D.   Modify the input filter on the network adapter for Subnet2. Configure the filter to receive only traffic that is responding to an existing session or is directed to TestKingRouter.

Answer: A
Explanation: The TestKingRouter filter exhibit shows that only the traffic with destination TestKingDNS and TestKingWeb is allowed from Subnet2 to Subnet1 (this is an Input filter on the Subnet 2 adapter). However, we must restrict the traffic from Subnet1 to Subnet2. We should only allow existing sessions, i.e. the sessions to TestKingDNS and TestKingWeb, and traffic to the router. We achieve this with an input filter on the Subnet 1 adapter.

Incorrect Answers
B: An output filter on the Subnet1 adapter as proposed in this solution would not let any traffic pass. At this point there are no existing sessions and TestKingRouter cannot be the source of an **output** filter on its own network adapters.
C: This solution also seems pretty good. It would only allow traffic corresponding to existing sessions to pass from Subnet1 to Subnet2. The existing sessions would be sessions to TestKingDNS and TestKingWeb initiated from Subnet2. It would be unnecessary to include routes directed to TestKingRouter in this filter as this is an output filter on an adapter on TestKingRouter. However, it would be more prudent to block the traffic before it is routed, namely as an input filter on Adapter1 instead of an output filter on Adapter2.
D: We already have an input filter for the Subnet2 adapter. We need filtering in both directions, not just from Subnet2 to Subnet1.

QUESTION NO: 278
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain testking.com and three sites. Each site is connected to the Internet by a T1 line. All sites are connected to each other by means of several Routing and Remote Access servers and through the Internet.

You install a Windows 2000 DNS server at each site. You need to ensure that client computers at each site can resolve the names of resources located at any other site. You also need to minimize the name resolution traffic that is passed though your Routing and Remote Access servers. In addition, you need to ensure that the DNS zone files cannot be altered by outside parties, and that all DNS records be managed on a single DNS server.

How should you configure each DNS server?

    A.   Add a standard primary zone to one DNS server.

             Add a standard secondary zone to reach of the other DNS servers.

             Configure the primary zone server to allow zone transfers only to the secondary zone servers.

    B.   Add a standard primary zone to each DNS server.

             Configure each server to allow zone transfers only to the other servers, and allow only secure dynamic updates.

    C.   Make each DNS server a member server in the Windows 2000 domain.

             Add an Active Directory integrated zone to each DNS server.

             Configure the servers to allow only secure dynamic updates.

    D.   Make each DNS server a domain controller in the Windows 2000 domain.

             Add an Active Directory integrated zone to one DNS server.

             Configure the DNS Server service to log on by using a domain user account.

Answer: A
Explanation: We implement a standard primary zone on one single DNS server and configure the other DNS servers with secondary zones. We only allow zone transfers from the primary zone to the other DNS servers. This achieves the requirements of this scenario:
- As we have a single domain we only need one zone to cover the name resolution for the domain. The secondary DNS servers receive full DNS zones through replication.
- It minimizes name resolution traffic. The local DNS servers will be used for name resolution. No name resolution traffic would pass over the WAN.
- Secondary servers cannot add zone records, so there is no risk that an outside party could change any DNS records. No DNS update traffic is replicated.

Incorrect Answers
B: A DNS zone can only have one single primary zone.

C: Member servers cannot host Active Directory zones. Domain Controllers would be required to host Active Directory integrated zones.

D: With only one single DNS server all name resolution traffic would have to be managed by this single server. All name resolution traffic would pass over the WAN connections and the RRAS servers. This is what we want to avoid.

QUESTION NO: 279
You are the administrator of the TestKing Winery network, which is configured as shown in the exhibit.
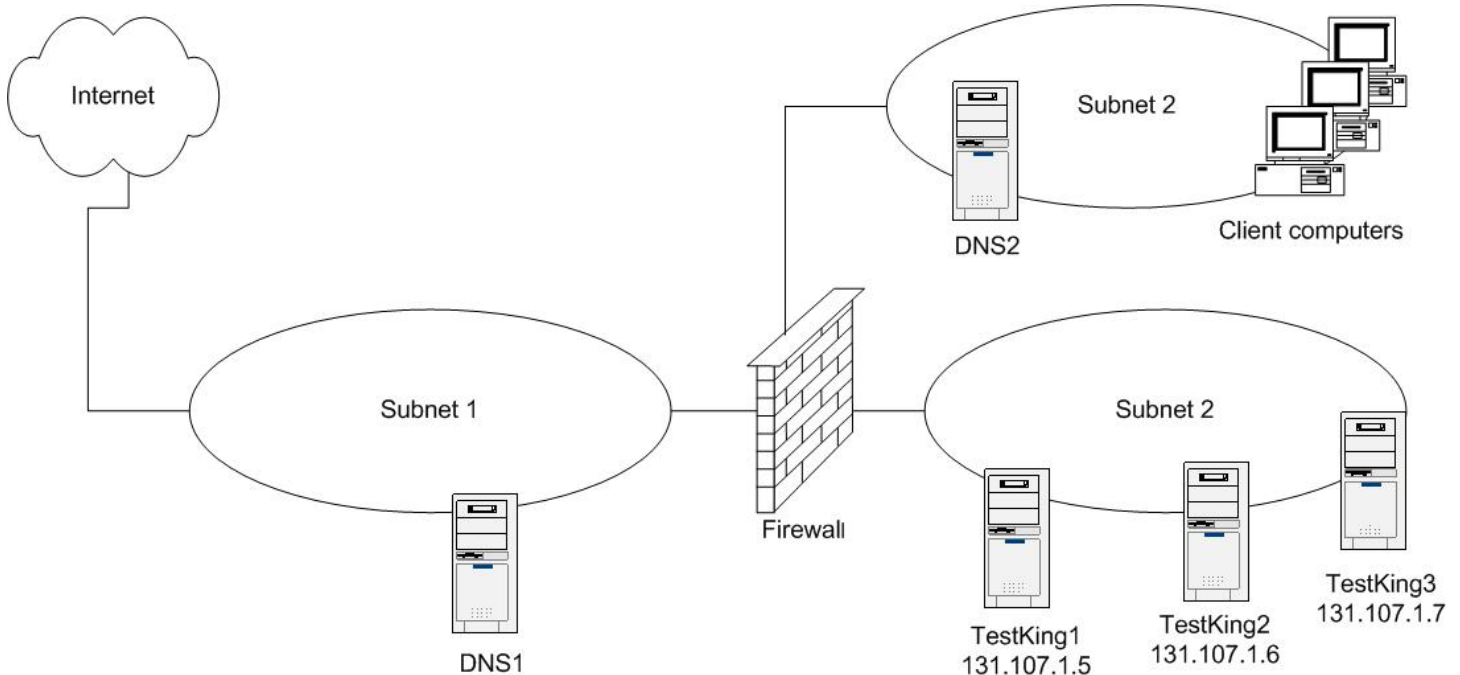
DNS1 and DNS2 are Windows 2000 Server computers running the DNS Server service. DNS2 hosts a standard primary zone for the internal company intranet. DNS2 is configured to use DNS1 as a forwarder.

TestKing1, TestKing2, and TestKing3 are Windows 2000 Server computers running Internet Information Services (IIS). All three Web servers host the company Web site, www.testking.com, and contain identical content. TestKing3 also hosts a secure Web site named TESTKINGWEB, which is used by company employees. Each Web server has a host record in the zone file on DNS1, which is used by administrators who need to access the Web servers for maintenance purposes.

You want to configure DNS1 to distribute the Web site traffic equally among all three Web servers. You also want DNS1 to resolve the name TESTKINGWEB.

You configure DNS1 to enable round robin DNS. How should you configure the zone file on DNS1?

To answer, click the Select and Place button, and then drag the correct DNS configuration parameters to the appropriate locations. You might need to use some parameters more than once.

Place here

Host Name	Record Type	IP address
		131.107.1.5
		131.107.1.6
		131.107.1.7

Host Name	Record type	Host alias

Select from these

Record types

A	PTR
CNAME	SRV

Host names or aliases

TestKing1	TestKing2	TESTKINGWEB
TestKing3	WWW	

Answer:

Place here

Host Name	Record Type	IP address
WWW	A	131.107.1.5
WWW	A	131.107.1.6
WWW	A	131.107.1.7

Host Name	Record type	Host alias
TestKing3	CNAME	TESTKINGWEB

Explanation: We add three A (host) records with the same host name with the IP addresses of the three web servers. We then add an alias record for TestKing3 since TestKing3 hosts the TESTKINGWEB web site.

Note: A canonical name (CNAME) record enables you to associate more than one host name with an IP address. This is sometimes referred to as aliasing. The following format is used for CNAME records:
hostname CNAME *aliasname*

QUESTION NO: 280
You are the administrator of TestKing's network, which is configured as shown in the exhibit.
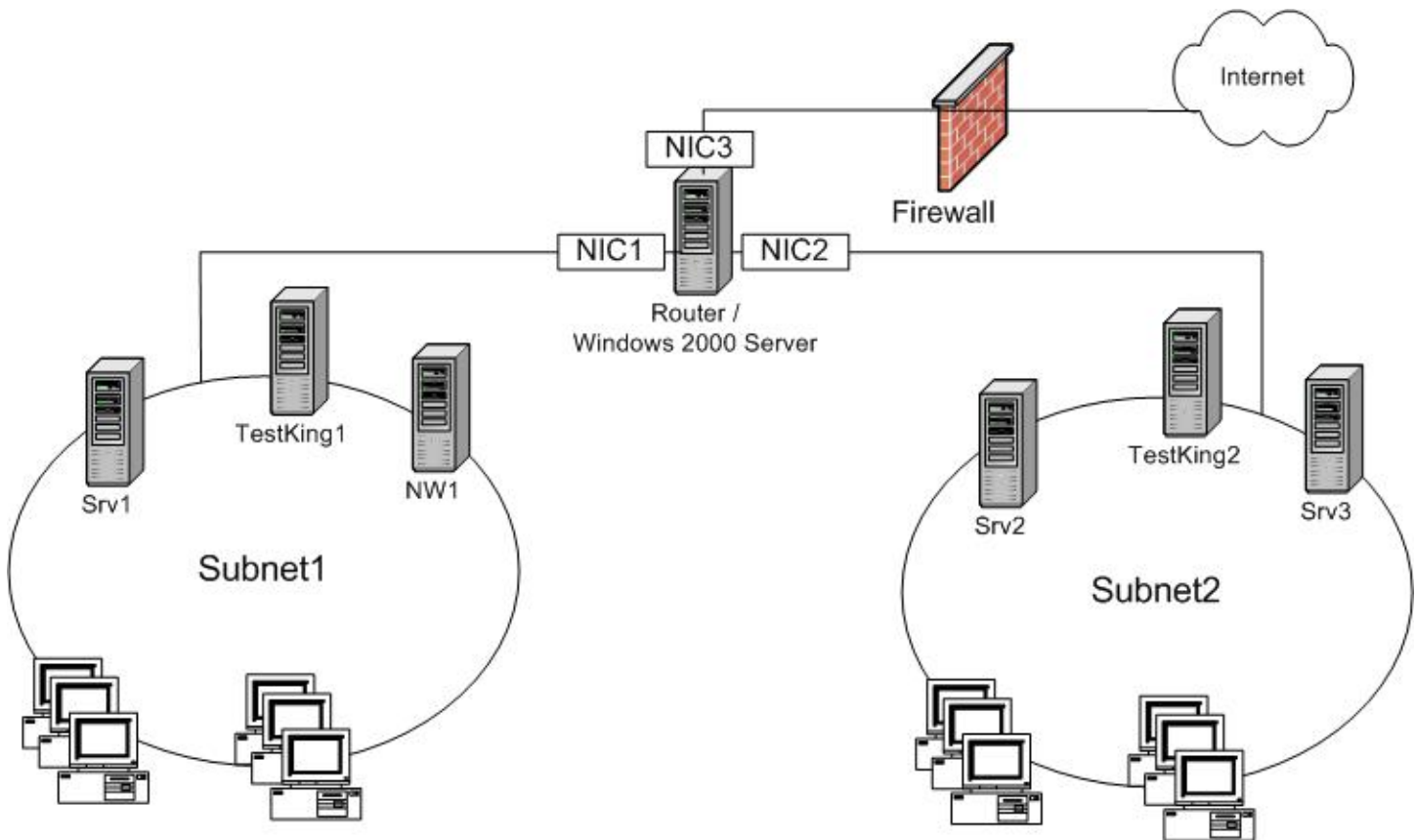
The router has three network adapters named NIC1, NIC2, and NIC3. Each subnet contains one Windows 2000 domain controller. The domain controllers are named TestKing1 and TestKing2. Each subnet also contains Windows 2000 member servers, which host applications and file and print resources. Subnet1 contains one NetWare 4.1 server named NW-1.

Users on each subnet need access to their local Windows 2000 member servers. Users on both subnets need access to NW-1. Mobile users require virtual private network (VPN) access from the Internet to the Windows 2000 member severs on both subnets.

You must adjust the network protocol bindings on the router to optimize performance for all network traffic.

What should you do?

To answer, drag the correct network protocols to the appropriate network interface in the correct order. You might need to use some network protocols more than once. Use the minimum number of necessary protocols.

Network protocols - select from these

IPX/SPX

TCP/IP

NetBEUI

DLC

QoS Packet Scheduler

Place here

NIC1

1
2
3

NIC2

1
2
3

NIC3

1
2
3

Answer:

Network protocols -
select from these

Place here

IPX/SPX

TCP/IP

NetBEUI

DLC

QoS Packet Scheduler

NIC1

1	TCP/IP
2	IPX/SPX
3	

NIC3

1	TCP/IP
2	
3	

NIC2

1	TCP/IP
2	IPX/SPX
3	

Explanation: We need both TCP/IP and IPX/SPX on both local interfaces (NIC1 and NIC2). TCP/IP will be the most used protocol so we should put it first. We only need TCP/IP on the Network Interface (NIC3).

Incorrect Answers
NetBEUI: There is no need for NetBEUI. NetBEUI is not routable and should only be used on LANs with a single subnet.
DLC: DLC is not routable. DLC might be used by some print devices and in some IBM environments.
QoS Packet Scheduler: QoS Packet Scheduler is a method of network bandwidth management that can monitor the importance of data packets and depending upon the priority of the packet, give it higher or lower priority or bandwidth levels. There is no use of **QoS Packet Scheduler** in this scenario.

QUESTION NO: 281
You are the administrator of TestKing's network, which serves one office with 150 users. The network includes 10 servers running Windows 2000 Server. All servers have static IP addresses. All client computers run Windows 2000 Professional and are DHCP clients.

A server named NATSvr1 provides Internet access by using the Network Address Translation protocol (NAT). NATSvr1 uses a pool of 100 IP addresses supplied by a contracted Internet service provider (ISP). A server named WebSvr1 hosts TestKing's Web site.

You need to improve remote access to WebSvr1 for 25 full-time employees who frequently work off-site. In addition, you need to provide remote access to WebSvr1 for five independent Web developers who work off-site and regularly update the company Web site. Your solution must involve the fewest possible changes to the configuration of NATSvr1.

Leading the way in IT testing and certification tools, www.testking.com

What should you do?

    A.   Move your company Web site to NATSvr1.
    B.   Map one of the ISP-assigned IP addresses directly to the IP address and port of WebSvr1.
    C.   Configure the remote computers to access WebSvr1 by using an L2TP/IPSec virtual private network (VPN).
    D.   Reassign 30 of the ISP-assigned IP addresses to remote users.
        Exclude these 30 addresses from the address pool.

Answer: B
Explanation: We should make a static mapping for the Web Server.

Incorrect Answers
A: Hosting the Web site on the NAT Server is generally not a preferred solution.
C: A L2TP/IPSec VPN would improve security, not performance.
D: We should not use the public IP addresses for the remote users.

QUESTION NO: 282
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain with two subnets. The relevant portion of your network configuration is shown in the exhibit.
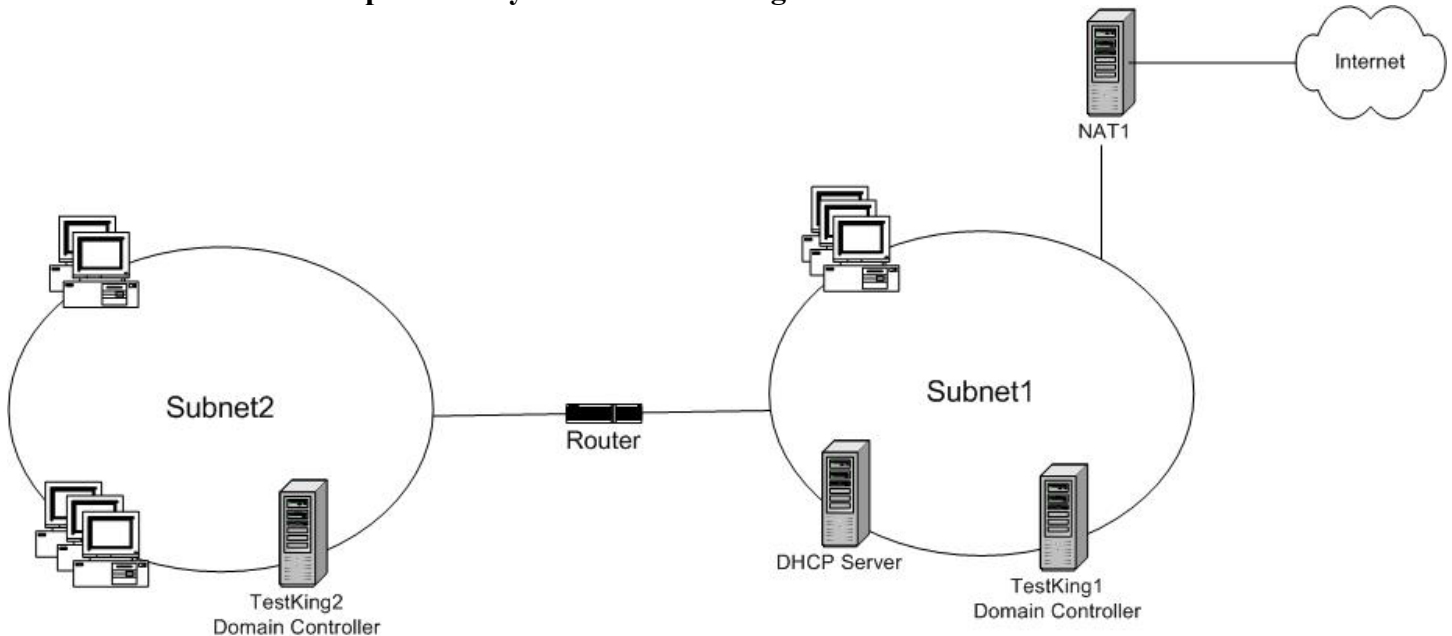
All client computers run either Windows 2000 Professional or Windows NT Workstation 4.0. All client computers on both subnets receive their TCP/IP configuration from the DHCP server.

Leading the way in IT testing and certification tools, www.testking.com

To enable users to access the Internet, you install Routing and Remote Access on a Windows 2000 Server computer named NAT1. You configure the Network Address Translation protocol (NAT) on NAT1.

Users in Subnet2 report that they cannot access the Internet. However, these users can access resources located on servers in Subnet1. Users in Subnet1 report no problems. On investigation, you discover that no client requests from Subnet2 are being received or processed by NAT1.

How should you correct this problem?

    A. Configure the router with a default route to the internal IP address of NAT1.
    B. Configure the router with a default route to the IP address of the router of your Internet service provider (ISO).
    C. Configure the Router scope option in DHCP to supply the internal address of NAT1 to the client computers in Subnet2.
    D. Configure the Router server option in DHCP to supply the internal address of NAT1 to all client computers.

Answer: A
Explanation: The clients on Subnet2 must gain internet access through the NAT Service. A default route to the internal interface of NAT1 would enable these clients to use the NAT service.

Incorrect Answers
B: A default route to the ISP would not give internet connectivity. We must go through the NAT Server.
C, D: The clients on Subnet2 can already access resources outside their local subnet. There is no need to reconfigure the Default Gateway (Router) option.

QUESTION NO: 283
You are the administrator of TestKing's network, which includes 200 Windows 2000 Professional computers and one Windows 2000 Server computer named TestKing1.

TestKing1 runs a custom client/server application. The application uses TCP/IP for communications. Client computers initially query TestKing1 on TCP port 4173. Subsequent communications occur on a randomly assigned port chosen by the client/server application.

The client/server application tracks confidential research data. You must ensure that this data is secure and encrypted when it is transmitted across the network.

You create a custom IPSec policy on TestKing1 that requires encrypted communications on TCP port 4173.
Which additional action or actions should you apply? (Choose all that apply)

    A. Configure the client computers with the Client IPSec policy.

Leading the way in IT testing and certification tools, www.testking.com

B. Configure the client computers with the Server IPSec policy.
C. Configure TestKing1 with the Server IPSec policy.
D. Configure TestKing1 with the Secure Server IPSec policy.

Answer: A, C
Explanation:
A: The Client (Respond Only) policy allows communications in plaintext but will respond to IPSec requests and attempts to negotiate security. This policy would ensure that the clients respond to the application requests using encrypted traffic.
C: The Server (Request Security) policy causes the server to attempt to initiate secure communications for every session. This would ensure that the client/server traffic would be encrypted.

Incorrect Answers
B: We don't want the clients to request security.
D: We are not required to encrypt all traffic to and from TestKing1, only the client/server application must be secured.

QUESTION NO: 284
You are the administrator of TestKing's network, which consists of a single switched network segment. The computers on your network have the characteristics shown in the following table.

Computer type	Number of computers	Operating system	Hardware vendor
Server	55	Windows 2000 Server	Vendor A
Client	250	Windows 2000 Professional	Vendor B
Client	70	UNIX	Mix of Vendor C and Vendor D

All Windows 2000 computers are configured as DHCP clients. All UNIX computers are configured as BOOTP clients. All Windows 2000 computers must use a server named WIDN1 for DNS services, and must also be assigned a WINS server. All Windows 2000 Professional computers must attempt to renew their DHCP leases after eight hours, and all Windows 2000 Server computers must attempt to renew their DHCP leases after 10 days. All UNIX computers must use a server named UNDN2 for DNS services.

You install a DHCP server on your network and configure it with four scopes. Now you need to configure this server to issue IP addresses and DHCP options to the appropriate computers.

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

A. Add a multicast scope range for the Windows 2000 Professional computers.
B. Define a user class for the UNIX computers.
C. Define a user class for the servers.
D. Define a vendor class for the Windows 2000 Professional computers.

Leading the way in IT testing and certification tools, www.testking.com

E. Define a vendor class for the servers.
F. Define and IP address reservation for the servers.
G. Define and IP address reservation for the UNIX computers.

Answer: B, D, E
Explanation:
B: With user classes, you can take advantage of predefined classes that can be used to support specialized groups of clients, such as BOOTP clients.
D: All Windows 2000 Professional computers are from the same vendor. We can therefore use a vendor class for these clients.
E: As all servers are from the same vendor we can use a vendor class.

Reference: Windows 2000 Server documentation, Understanding user and vendor classes

Note: User Classes assign DHCP options to a group of clients that require similar configuration; Vendor Classes typically assign vendor-specific options to clients that share a common vendor type.

Incorrect Answers
A: Multicast is not called for in this scenario.
C: It would require less administration to use a vendor class.
F, G: IP address reservations would require too much administration.

QUESTION NO: 285
You are a consultant hired by Adventure Works, a small company that specializes in unusual vacations. Adventure Works enters into a partnership with Alpine Ski House, TestKing's Travel, and Blue Yonder Airlines to provide exotic ski vacations.
Adventure Works sells the vacation packages and resells ski equipment manufactured by Alpine Ski House. TestKing's Travel makes flight reservations on Blue Yonder Airlines and books hotel reservations. Adventure Works coordinates all aspects of the partnership.

Each company's network consists of a single Windows 2000 domain. Each domain includes a single domain controller running Windows 2000 Server. The domain controllers are named ASH-DC, AW-DC, BYA-DC, and TK-DC. Each one runs the DNS Server service and hosts an Active directory integrated zone.

The four networks are connected over the Internet by means of persistent virtual private network (VPN) connections. The relevant portion of the network configuration is shown in the exhibit.

Leading the way in IT testing and certification tools, www.testking.com
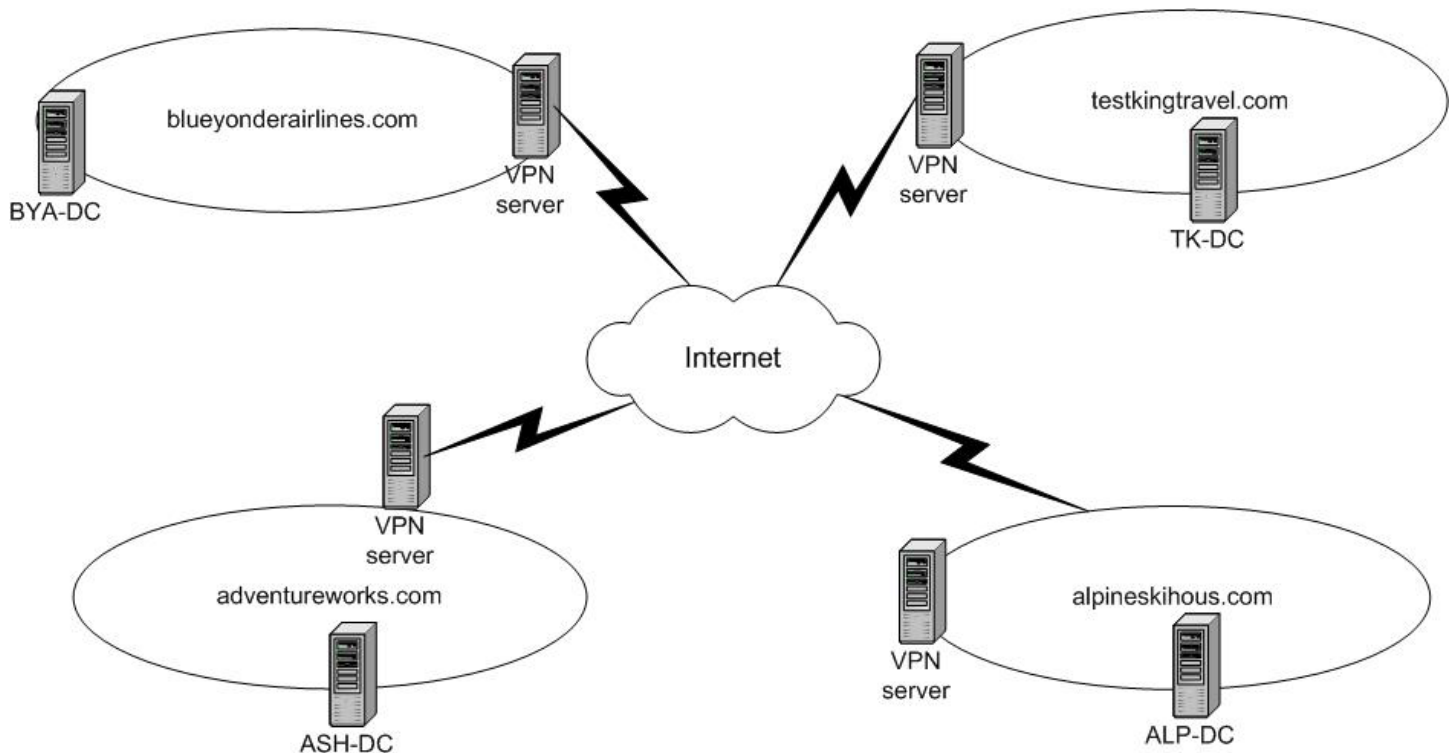
Users at Adventure Works require access to applications and resources in the networks of all three partners. Users at TestKing's Travel require access to applications and resources in the Blue Yonder Airlines network. However, users at Adventure Works and TestKing's Travel report that they often receive an error message when they try to access servers located on the other networks. The error message states:

"Network path could not be found."

To correct this problem, you install the DNS Server service on new stand-alone servers running Windows 2000 Server in the Adventure Works network and the TestKing's Travel network.

How should you configure DNS in these two networks?

Drag the correct DNS configuration parameter to the appropriate DNS server. You might need to use some parameters more than once.

Create Zone Type   **Zone Name**   **Zone Types**

	alpinskihouse.com	Primary

AW-DNS

	blueyonderairlines.com	Secondary

	testkingtravel.com	Active Directory Integrated

TK-DNS

	blueyonderairlines.com

Forwarder   **Possible forwarders**

AW-DNS

AW-DC	ASH-DC
BYA-DC	TK-DC
AW-DNS	TK-DNS

TK-DNS

Answer:

Create Zone Type	Zone Name	Zone Types
Secondary	alpinskihouse.com	Primary
Secondary	blueyonderairlines.com	Secondary
Secondary	testkingtravel.com	Active Directory Integrated
Secondary	blueyonderairlines.com	

AW-DNS

TK-DNS

Forwarder

AW-DNS — TK-DC

TK-DNS — BYA-DC

Possible forwarders

AW-DC   ASH-DC

BYA-DC

AW-DNS   TK-DNS

Explanation: We only need read-only replicas of the zone. We should use secondary zones.
As forwarder we should use the DNS server that is authoritative for the zone – the domain controller. For the Adventureworks DNS server we should use the Domain Controller in the testkingtravel.com zone.
For the TestKing's Travel DNS server we should use the Domain Controller in the blueyonderairlines.com zone.

QUESTION NO: 286
You are the administrator of TestKing's network, which links the main office and 15 branch offices. The network contains 5,000 computers running Windows 2000 Professional and 180 computers running Windows 2000 Server.

The main office has two WINS servers, and each branch office has one WINS server. The WINS servers in the branch offices are configured for push/pull replication with one of the WINS servers in the main office. Both WINS servers in the main office are configured for push/pull replication with each other.

You enable periodic database consistency checking. You then notice an increase in network traffic during the check periods. You need to reduce or eliminate the additional traffic, while maintaining the integrity of the database records.

What should you do?

 A. Configure all WINS servers to use the automatic partner configuration.
 B. Disable periodic database consistency checking and manually perform consistency checking.
 C. Increase the verification interval on each of the WINS servers.
 D. Configure the DHCP client options for WINS so that the primary WINS servers are evenly divided among the DHCP clients.

Answer: C
Explanation: The WINS verification interval specifies the time after which the WINS server must verify that old names that it does not own are still active. By increasing this interval network traffic would be reduced.

Note: During each scheduled consistency check, the selected WINS server compares local copies of records it stores with the same records stored on the WINS server listed as the owner for each record.

Incorrect Answers
A: Automatic partner configuration is recommended only if you have a small number of installed WINS servers (typically, three or fewer) on the reachable network.
B: This would require additional administration.
D: This would distribute work load between WINS clients. It would not reduce network traffic during database consistency checking.

QUESTION NO: 287
You are the network administrator for TestKing. The network consists of 20 network segments connected by a router. One segment includes all the server computers. Each other segment includes 50 Windows 2000 Professional client computers.

You install a new Windows 2000 Server computer named ServerA on the server segment. You install and configure the DHCP Server service on TestKingSrv.

You decide to use one of the client computer segments as a test segment. You create and configure a scope for the test segment, and you configure the client computers on that segment so that each client computer uses DHCP to obtain its IP configuration. You configure the scope to use a Class C subnet mask.

Leading the way in IT testing and certification tools, www.testking.com

Users on the test segment immediately report that they cannot access server-based resources.

You need to ensure that the client computers on the test segment can connect to server-based recourses.

You open the DHCP console. Which DHCP setting or settings should you modify or delete? (Choose all that apply)

To answer, select the appropriate setting or settings in the dialog box.

Address Pool		
Start IP Address	End IP Address	Description
192.168.50.2	192.168.50.250	Address range for distribution

Answer: Unable to answer without complete exhibit.
Possibly the default gateway setting is incorrect.

QUESTION NO: 288
You are the network administrator for the TesKing Corporation, whose URL is www.testking.com. Your network consists of a single Windows 2000 domain. It includes a Windows 2000 Server computer named Files1 and a DNS server named DNS1. Files1 contains several shared folders. DNS1 is configured to allow dynamic updates.

According to company policy, all data transmitted across the network must be protected from interception by unauthorized individuals. To comply with this policy, you apply the default Client IPSec policy to all client computers. You also apply the default Secure Server IPSec policy to Files1.

Users report that they can no longer access shared folders on Files1. You verify that client computers can connect to other network servers and to each other. When you run the ping files1.testking.com command, you receive the following error message: "Unknown host files1.testking.com". However, you can successfully ping the IP address of Files1.

You need to enable users to access the shared folders on Files1. You must maintain the highest possible level of network security. What should you do?

A.   On the client computers, create a custom IPSec policy that exempts DNS traffic between client computers and DNS1.
B.   On DNS1, add CNAME (canonical name) records for Files1.
C.   On DNS1, create a custom IPSec policy that exempts DNS traffic between Files1 and DNS1.
D.   On Files1, install a server encryption certificate.
     Configure the client computers to trust the certificate authority that issued the server encryption certificate.

Leading the way in IT testing and certification tools, www.testking.com

Answer: C
Explanation: We must allow Files1 to be dynamically registered on DNS1. This will allow the clients to access Files1 using a host name.

QUESTION NO: 289
You are the administrator of TestKing's network, which consists of a single Active Directory domain. All servers on the network run Windows 2000 Server and all client computers run Windows 2000 Professional. Many employees work at home while using personally owned desktop computers. A large sales staff travels extensively while using company-issued portable computers.

You need to set up remote access server that will enable all these users to access network resources. For security, you plan to implement Routing and Remote Access client connections by using an L2TP/IPSec tunnel for all remote users.

You install and configure Routing and Remote Access and configure a virtual private network (VPN) server. You accept all default settings for an L2TP tunnel configuration on the Internet interface. You install a computer running Microsoft Certificate Server on the network. You configure the VPN connection objects for the users of portable computers. You instruct the home-based users to configure their connections by using the Network Connections wizard on their desktop computers.

Home-based users now report that they cannot connect to the network through the new VPN server. The sales staff reports no problem.

You must provide all remote users with secure access to network resources. What should you do?

    A.   Instruct the home-based users to obtain certificates from the certificate server's Internet enrollment site.
    B.   Configure the home-based computers with a pre-shared key for authentication.
    C.   On the home-based computers, assign the Client (Respond Only) IPSec policy.
    D.   On the home-based computers, assign the Server (Request Security) IPSec policy.

Answer: A
Explanation: The Windows Server family supports two authentication methods for Layer Two Tunneling Protocol over Internet Protocol security (L2TP/IPSec)-based VPN connections: computer certificates, also known as machine certificates, and preshared keys.
In order to create an L2TP/IPSec connection using the computer certificate authentication method, you must install a certificate in the local computer certificate store on the VPN client and VPN server computer. To install a computer certificate, a certification authority must be present to issue certificates. Once the certification authority is configured, you can install a certificate in three different ways:

- By configuring the automatic enrollment, or auto-enrollment, of computer certificates to computers in a Windows 2000 domain.
- By using the Certificates snap-in to obtain a computer certificate.
- By using your browser to connect to the CA Web enrollment pages to install a certificate on the local computer or to a floppy disk for installation on another computer, such as a user's home computer.

Reference: Basic L2TP/IPSec Troubleshooting in Windows

Incorrect Answers
B: Not the best solution.
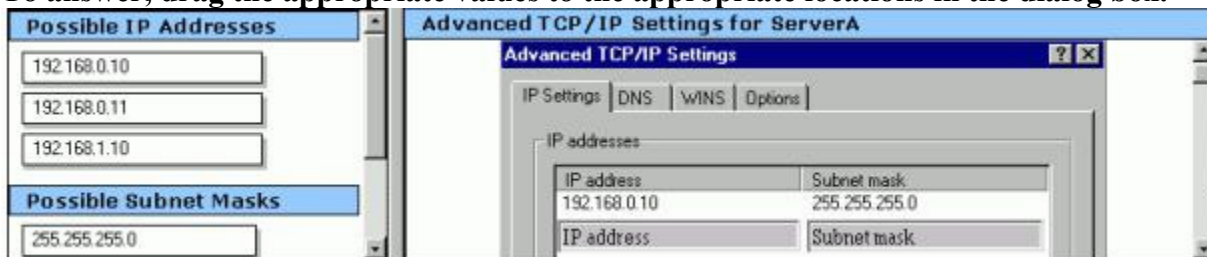**C, D:** This is not IPSec policy issue.

QUESTION NO: 290
You are the network administrator for TestKing. The network consists of 12 network segments connected by a router. All server computers are located on a single segment. The server segment includes a Windows 2000 Server computer named TestKingSrv. TestKingSrv runs Internet Information Services (IIS) and is configured to host a single Web site.

The Web developers in your company configure TestKingSrv to host an additional Web site. Users will access the new Web site by using a dedicated IP address. The developer asks you to configure the TCP/IP settings on TestKingSrv to support the new Web site.

How should you configure the TCP/IP properties for TestKingSrv?
To answer, drag the appropriate values to the appropriate locations in the dialog box.

Possible IP Addresses	Advanced TCP/IP Settings for ServerA
192.168.0.10	**Advanced TCP/IP Settings** ? ☒
192.168.0.11	IP Settings │ DNS │ WINS │ Options │
192.168.1.10	IP addresses
Possible Subnet Masks	IP address — Subnet mask
255.255.255.0	192.168.0.10 — 255.255.255.0
	IP address — Subnet mask

Answer:
IP address	Subnet mask
192.168.0.10	**255.255.255.0**
IP address	**Subnet mask**
192.168.0.11	255.255.255.0

Explanation: The exhibit shows that the server is using 192.168.0.10 as its IP address. To access the second website using a dedicated IP address, we must add an IP address from the same range as the 192.168.0.10 address. From the choices given, the only IP address in the same range is 092.168.0.11.

The subnet mask must be the same for both IP addresses; in this case: 255.255.255.0.

QUESTION NO: 291
You are the network administrator for TestKing. The network consists of a Windows 2000 Active Directory domain running in native mode. The domain includes a Windows 2000 Server computer named TestKingSrv. TestKingSrv runs Routing and Remote Access and is configured as a dial-up server only. TestKingSrv uses remote access polices to control dial-up access. TestKingSrv is a member of the domain.

A user named Nina reports that she is never able to connect to TestKingSrv by using her Windows 2000 Professional computer. Whenever she tries, she receives the following message: "Access denied".

You verify that all other users in the company are able to connect to TestKingSrv by using their Windows 2000 Professional computers. You also verify that the remote access policies are configured to allow all users to dial in.

You need to ensure that Nina can dial in to TestKingSrv and access company resources in accordance with the remote access polices on TestKingSrv.

What should you do?

   A.   Configure TestKingSrv to accept MS-CHAP authentication.
   B.   Configure Nina's domain user account so that it uses remote access polices to control dial-up access.
   C.   Configure TestKingSrv to accept EAP authentication.
   D.   Configure Nina's computer to use a VPN connection to connect to TestKingSrv over the Internet.

Answer: B
The "Access Denied" error message indicates a permissions problem. The question states that the remote access policy gives the necessary permissions. Therefore, it is likely that Nina's account is not configured to use the remote access policy; her dial-in permission is set to "No Access". This needs to be changed to "Controlled by remote access policy".
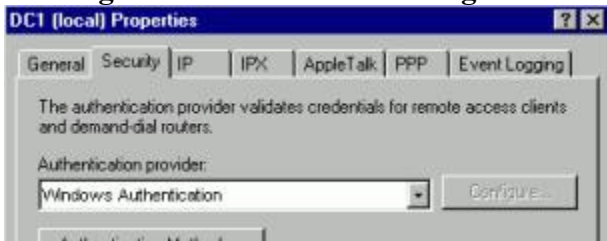
QUESTION NO: 292
You are the network administrator for TestKing. The network includes a Windows 2000 Server computer named DC1. DC1 runs Routing and Remote Access and is configured as a dial-up server. DC1 is also a domain controller.

You install a new Windows 2000 Server computer named TestKingSrv. You install and configure Internet Authentication Service (IAS) on TestKingSrv. You want to configure DC1 to use TestKingSrv to authenticate dial-up users and to record a log of dial-up activity.

How should you configure the properties of DC1?
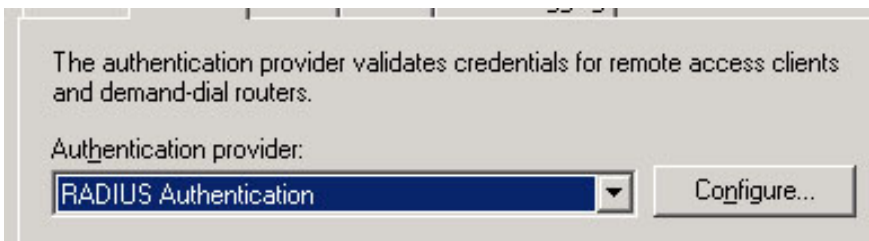**To answer, use the dialog box controls to configure the options correctly.**
Routing and Remote Access configuration for DC1

DC1 (local) Properties

General | Security | IP | IPX | AppleTalk | PPP | Event Logging

The authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication provider:

Windows Authentication

Configure...

Answer: Change the "Authentication provider" to "RADIUS authentication".

Explanation: IAS is Microsoft's implementation of a RADIUS server. To configure a remote access server to use a RADIUS server to authenticate users, we must change the "Authentication Provider" from "Windows Authentication" to "RADIUS Authentication".
To do this, open the drop down box for the Authentication Provider and select "RADIUS Authentication" from the list. See exhibit below:

The authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication provider:

RADIUS Authentication

Configure...

QUESTION NO: 293
You are the administrator of TestKing's network, which consists of a singe Windows 2000 domain. The network includes a stand-alone Windows 2000 Server computer named RAS1, which runs Routing and Remote Access. All employees use computers running Windows 2000 Professional to dial in to the network.

Your remote access polices permit members of the Domain Users group to dial in to RAS1 between 7:00 P.M and 6:00 A.M. every day. To increase dial-up security, your company issues smart cards to all employees.

You need to configure RAS1 and your remote access polices to support the use of the smart cards for dial-up connections.

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

Leading the way in IT testing and certification tools, www.testking.com

A.   Create a remote access policy that requires users to authenticate by using the EAP-TLS.
B.   Create a remote access policy that requires users to authenticate by using the MS-CHAP v2.
C.   Create a remote access policy that requires users to authenticate by using SPAP protocol.
D.   Add RAS1 to the Windows 2000 domain.
E.   Install the Internet Authentication Service (IAS) on RAS1.
F.   Install Certificate Services on RAS1 and configure it to issue encryption certificates upon request.

Answer: A, F
Explanation: To use Smart Cards for authentication, the remote access server must be configured to support EAP-TLS. We must also install Certificate Services on the server and configure it to issue encryption certificates upon request.

QUESTION NO: 294
You are the network administrator for TestKing International. The TestKIng network consists of a main office network and a branch office network. The offices are connected by a 256-Kbps Frame Relay connection.

The TestKing network includes two Windows 2000 Server computers named DC1 and DC2. Both DC1 and DC2 are configured as domain controllers and as WINS servers. DC1 is located in the main office and DC2 is located in the branch office.

All computers in the main office are configured to use DC1 as their only WINS server. All computers in the branch office are configured to use DC2 as their only WINS server.

Users in the branch office frequently access file servers located in the main office. However, users in the main office never access file servers located in the branch office,

You want to configure WINS replication between DC1 and DC2. You need to ensure that client computers in the branch office are able to access the file servers located in the main office by name. Make the appropriate configuration.

Partner Properties for DC2
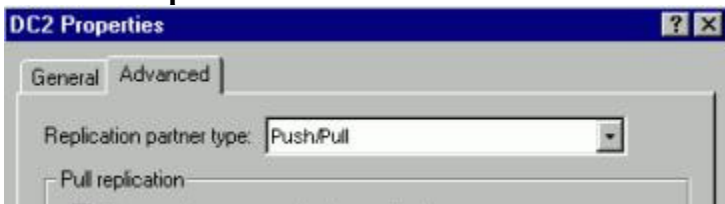
Answer: The clients in the branch office require access to files on the server in the main office. Therefore, the branch office WINS server (DC2) needs a copy of the WINS database from the main office WINS server

Leading the way in IT testing and certification tools, www.testking.com

(DC1). We should configure DC2 to be a "Pull" partner to DC1. This will enable DC2 to 'pull' a copy of the WINS database from DC1 at specified intervals. To do this, select the drop down box and select "Pull". See exhibit below:
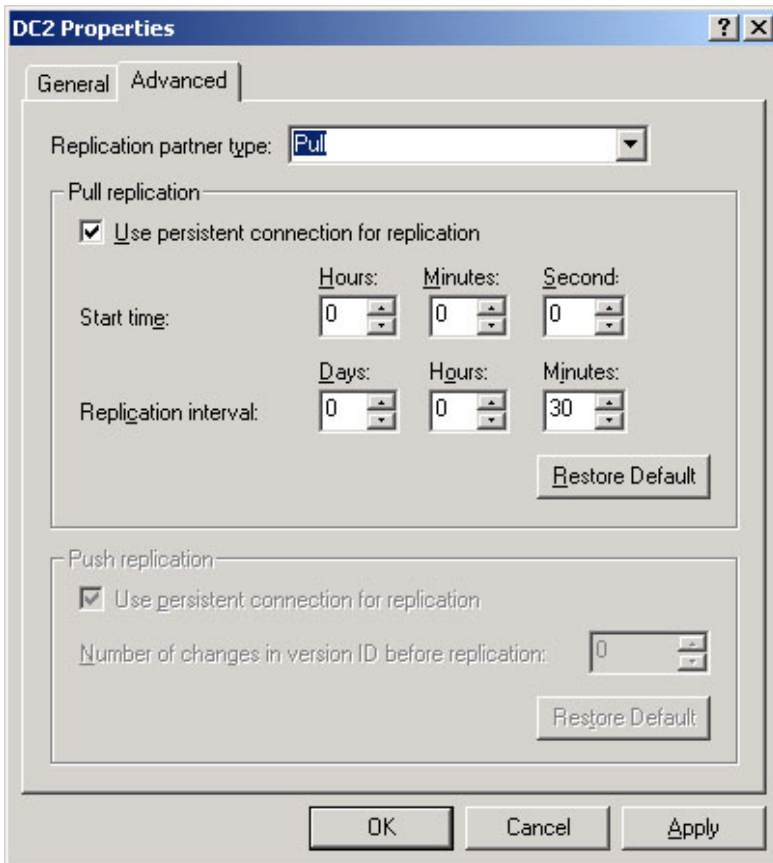
QUESTION NO: 295
You are the network administrator for TestKing. The network consists of three segments. Segment 1 and Segment 2 are connected by a Windows 2000 Server computer named TestKingA. Segment 2 and Segment 3 are connected by a router. TestKingA runs Routing and Remote Access. TestKingA is also connected to the company's firewall and routes traffic between network client computers and the Internet. The relevant portion of the network configuration is shown in the exhibit.
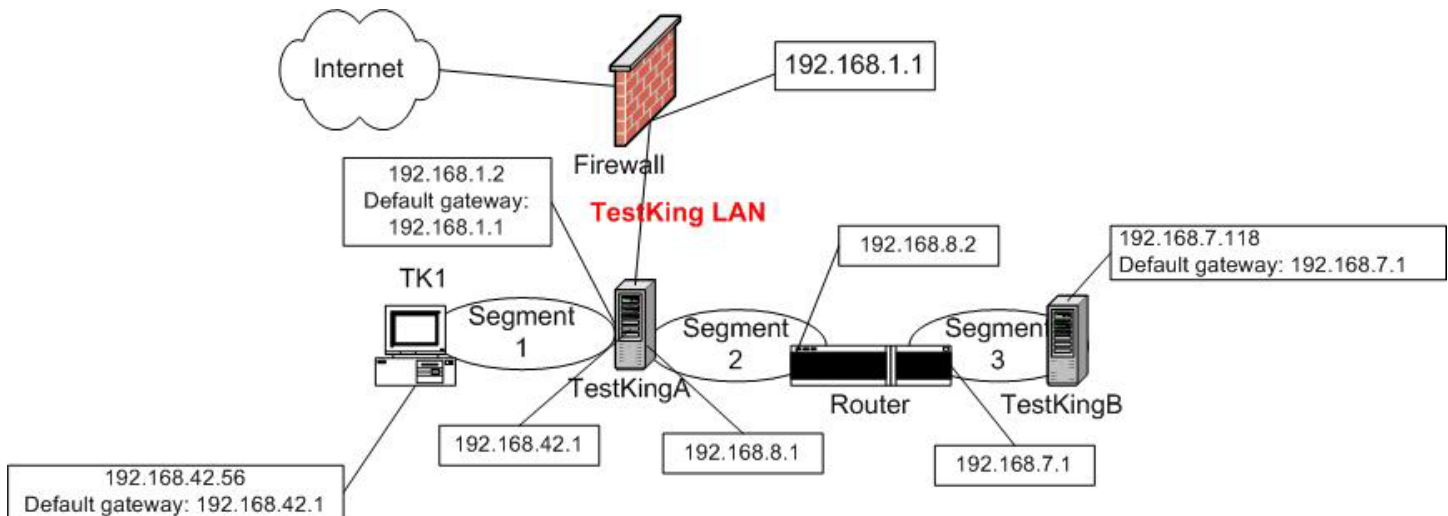
A Windows 2000 Professional computer named TK1 needs to send UDP-based traffic to a custom application running on a Windows 2000 Server computer named TestKingB. However, the log files for the application indicate that not traffic is being received from TK1.

You need to ensure that TestKingA is routing traffic from TK1 to the network segment that contains TestKingB.

You decide to create a static route on TestKingA to correct the problem. How should you create the route?

To answer, use the dialog box controls to configure the options correctly. Drag the appropriate value or values to the appropriate locations.
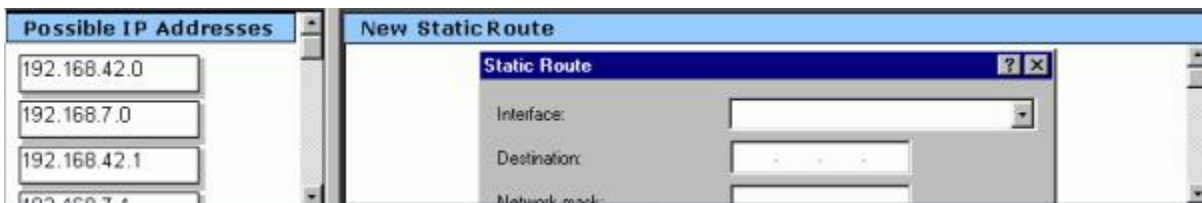
Answer:

Explanation: We need to add a static route from TestkingA to segment 3. The IP address of segment 3 is 192.168.7.0. This should be entered for the "Destination".
192.168.7.0 is a Class C network address; therefore we should enter 255.255.255.0 for the "Network mask"
The Gateway is the local interface of router that connects subnet 2 to subnet 3. Therefore, we should enter 192.168.8.2 for the "Gateway". This tells Testking A that any traffic destined for subnet 3 should be forwarded to 192.168.8.2 (the router that connects to subnet 3).
It's difficult to know what the exact entry for the "Interface" should be without seeing the complete exhibit. The answer should be the interface that connects to subnet 2 (the interface with the IP address 192.168.8.1). In the answer exhibit, I've selected Local Area Connection 2. In the exam, this might have been renamed to reflect the IP address 192.168.8.1. So if 192.168.8.1 is an option, then that should be entered for the "Interface".

QUESTION NO: 296
You are the administrator of TestKing's network. You install a multihomed server running Windows 2000 Server to functions as management server. The relevant portion of the resulting network configuration is shown in the exhibit.
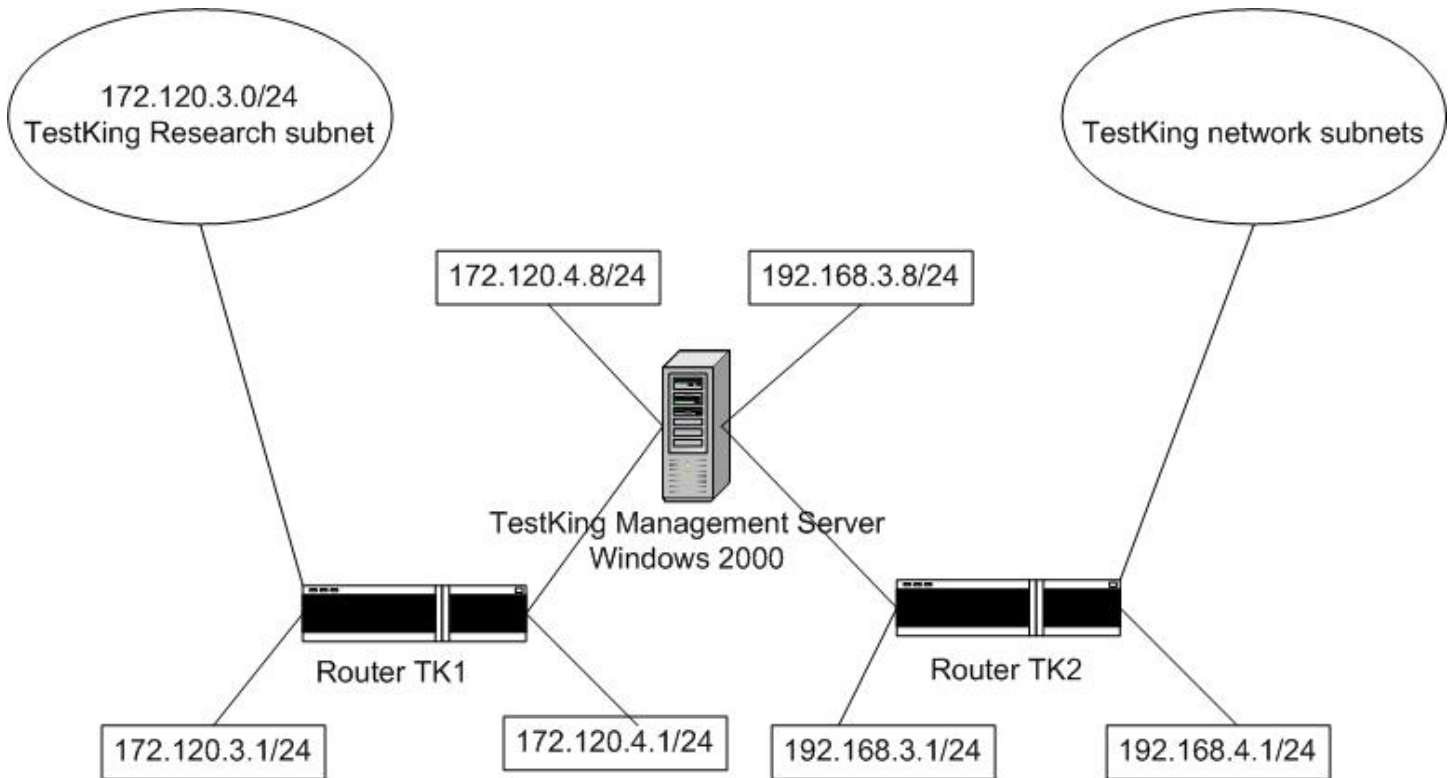
TestKing maintains a research subnet that contains 75 computers. The research subnet is completely separate from the rest of the network.

You need to configure the management server to communicate with all hosts and all subnets. However, the research subnet must not be able to communicate with the company network subnets.

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

- A. Configure the management server with a default gateway of 192.168.3.1
- B. Configure the management server with a default gateway of 172.120.3.1
- C. Run the **route add 172.120.3.0 MASK 255.255.0.0 172.120.4.1 –p** command.
- D. Run the **route add 172.120.3.0 MASK 255.255.255.0 172.120.4.1 –p** command.
- E. Run the **route add 192.168.3.1 MASK 255.255.255.0 192.168.4.1 –p** command.
- F. Run the **route add 192.168.3.1 MASK 255.255.0.0 192.168.4.1 –p** command.

Answer: A, C
Explanation: By configuring the management server with a default gateway of 192.168.3.1, all traffic destined for a remote network will be forwarded to 192.168.3.1. This will enable the management server to communicate with the Testking network subnets.
However, to communicate with the Testking Research subnet, we must add a static route, so that traffic destined for the Research subnet is forwarded to the appropriate router. We can do this with the command: **route add 172.120.3.0 MASK 255.255.0.0 172.120.4.1 –p**

The command says that any traffic destined for the 172.120.3.0 (Research) subnet will be forwarded to 172.120.4.1 instead of the default gateway. 172.120.4.1 is a Class B address so the subnet mask is 255.255.0.0. The "-p" makes the route "persistent", meaning that the route is still there if the machine is rebooted.

Incorrect Answers:
B: There are multiple subnets connected to the 192.168.3.1 router and only one subnet connected to the 172.120.3.1 router. Furthermore, the default gateway must be the local interface of a router. 172.120.3.1 is the external interface of the router.
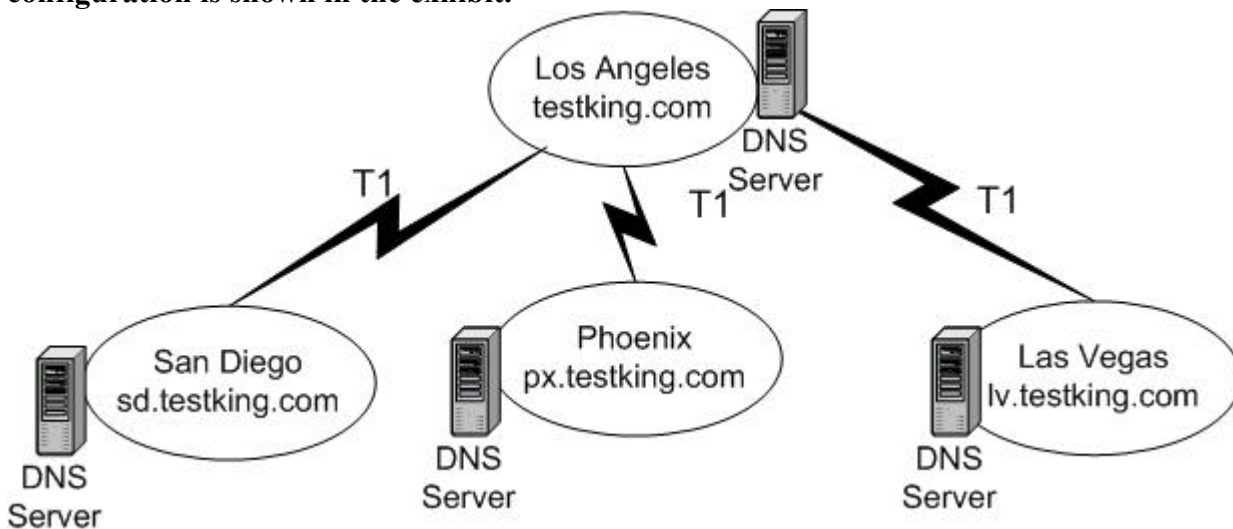**D:** 172.120.x.x is a class B address. This answer has a class C subnet mask.
E: This static route is routing to the wrong network.
F: This static route is routing to the wrong network.

QUESTION NO: 297
You are the network administrator for TestKing, Inc. The relevant portion of your network configuration is shown in the exhibit.

Los Angeles
testking.com
DNS Server
T1   T1   T1
San Diego
sd.testking.com
DNS Server
Phoenix
px.testking.com
DNS Server
Las Vegas
lv.testking.com
DNS Server

Your network includes four LANs: one at your main office and one at each of your three branch offices. Each office has its own Windows 2000 domain with approximately 500 users. Each office also contains one domain controller for the local domain.

Users at the branch offices report extremely slow response times when they try to access resources located at the Los Angeles office. On investigation, you discover that each request for name resolution takes several minutes.

You need to improve access times. You also want to minimize the amount of T1 bandwidth used by name resolution. What should you do?

Leading the way in IT testing and certification tools, www.testking.com

A.   Configure the DNS server in each branch office to forward requests to the DNS server in Los Angeles.
B.   Configure a caching-only DNS server at each branch office.
C.   On all client computers at each branch office, create a Hosts file and configure it with the name and IP address of the DNS server in Los Angeles.
D.   On the DNS servers at each branch office, create a standard secondary zone for the testing.com domain.
        Configure zone transfers to occur during non-business hours.
E.   Create an Active Directory integrated zone for all four domains.
        Configure the zone to replicate the zone database during non-business hours.

Answer: D.
Explanation: When a client in a branch office tries to access a resource in the main office, the DNS resolution request is forwarded over the WAN link to the DNS server at the main office. We can improve name resolution times by configuring the branch office DNS servers to have a copy of the zone file from the main office DNS server. We do this by creating a standard secondary zone for the testking.com domain on the DNS servers in each branch office.

Incorrect Answers:
A: The requests are already being forwarded to the DNS server in Los Angeles. This is what is causing the delay.
B: This could work, but until every resource has requested, resolved and cached, the delays will still occur. This is therefore, not the best solution.
C: This would be an administrative nightmare.
E: We have four domains. You must have one zone per domain – you cannot have one zone for all four domains.

QUESTION NO: 298
You are the administrator of TestKing's network, which consists of a single Windows 2000 domain and four sites, as shown in the exhibit.
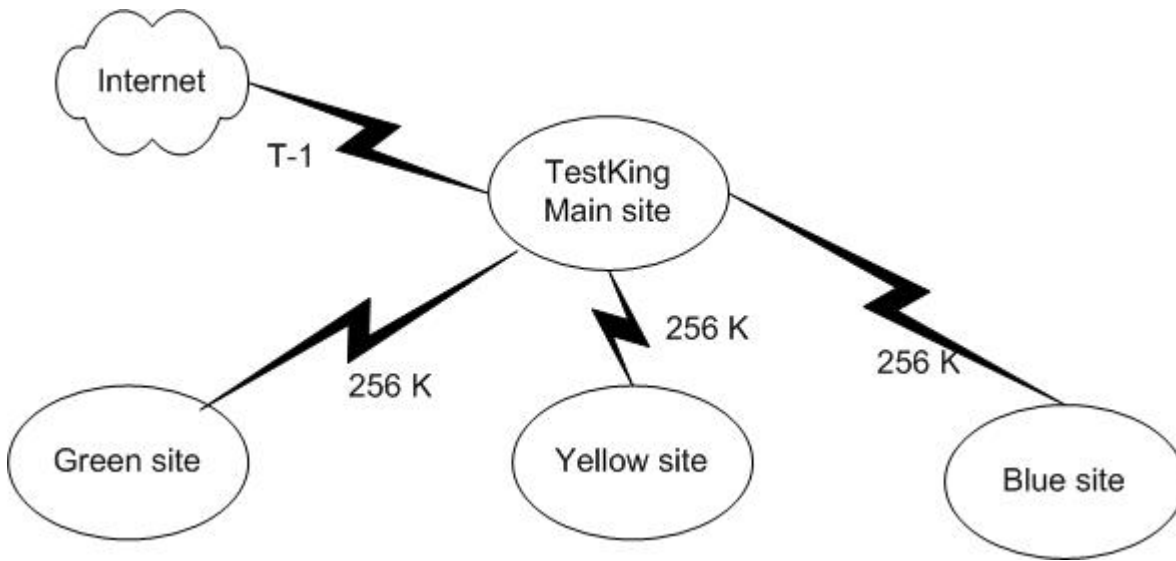
Each site contains a domain controller for the domain. You install the Windows 2000 DNS Server service on each domain controller.

Now you need to ensure that the client computers at each site can resolve the names of resources located at all other sites. Because the inter-site links receive heavy usage, you want to minimize name resolution traffic between sites. In addition, you want to ensure that the DNS zone files cannot be altered by outside parties, and that all DNS records can be managed from any DNS server.

How should you configure each DNS server?

    A.   Create a standard primary zone on the DNS server at the TestKing Main site.
            Add a standard secondary zone to each of the other DNS servers in the other sites.
            Configure the primary zone server to allow zone transfers only to the secondary zone servers.
    B.   Create a standard primary zone on each DNS server in each site.
            Configure each server to allow zone transfers only to the other servers, and to allow only secure dynamic updates.
    C.   Create an Active Directory integrated zone on the DNS server at the TestKing Main site.
            Add a standard secondary zone to each of the other DNS servers in the other sites.
            Configure the Active Directory integrated zone server to allow zone transfers only to the secondary zone servers.
    D.   Create an Active Directory integrated zone on each DNS server in each site.
            Configure the servers to allow only secure dynamic updates.

Answer: D.
Explanation: DNS servers configured with an Active Directory Integrated zone are "multi-master". This means that the DNS records can be managed from any DNS server. Replication between AD integrated zones uses IXFR (incremental updates). This means that only DNS records that have changed are replicated, thus

Leading the way in IT testing and certification tools, www.testking.com

reducing replication traffic. Allowing only secure dynamic updates will ensure that DNS records cannot be altered by outside parties.

Incorrect Answers:
A: DNS records can only be managed at a primary server; they cannot be managed at a secondary server. The question states that DNS records must be managed at any server.
B: You can have only one standard primary per domain.
C: DNS records can only be managed at a primary server; they cannot be managed at a secondary server. The question states that DNS records must be managed at any server.

QUESTION NO: 299
You are the network administrator for Contoso, Ltd. The network includes a Windows 2000 Server computer that is configured as a DNS server. The DNS server provides DNS name resolution services for Internet users and is configured to use round robin.

Another administrator installs a new Internet Web server named Web1. The server is configured to host two Web sites, which users will access by using the following URLs: http://team and http://intranet. The IP address of Web1 is 192.168.17.5. The administrator creates a DNS A (host) records for Web1.

You need to configure the DNS server so that users can connect to the new Web sites by using the appropriate URLs.

Which DNS records type should you create?
To answer, drag the appropriate record types, hosts, and aliases to the appropriate type, hosts, and alias boxes.

Answer:

CNAME   web1.contoso.com   team
CNAME   web1.contoso.com   intranet

Explanation: We need to 'map' the urls http://team and http://intranet to the webserver which is named web1.contoso.com. We do this with CNAME records. The host is the name of the webserver – this must be a host name, not an IP address. The Aliases are "team" and "intranet".