



[www.chinatag.com](http://www.chinatag.com)

**CHINATAG**

70-216

Implementing and Administering a Microsoft  
Windows 2000 Network Infrastructure

Q&A

DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are not encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

## **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.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

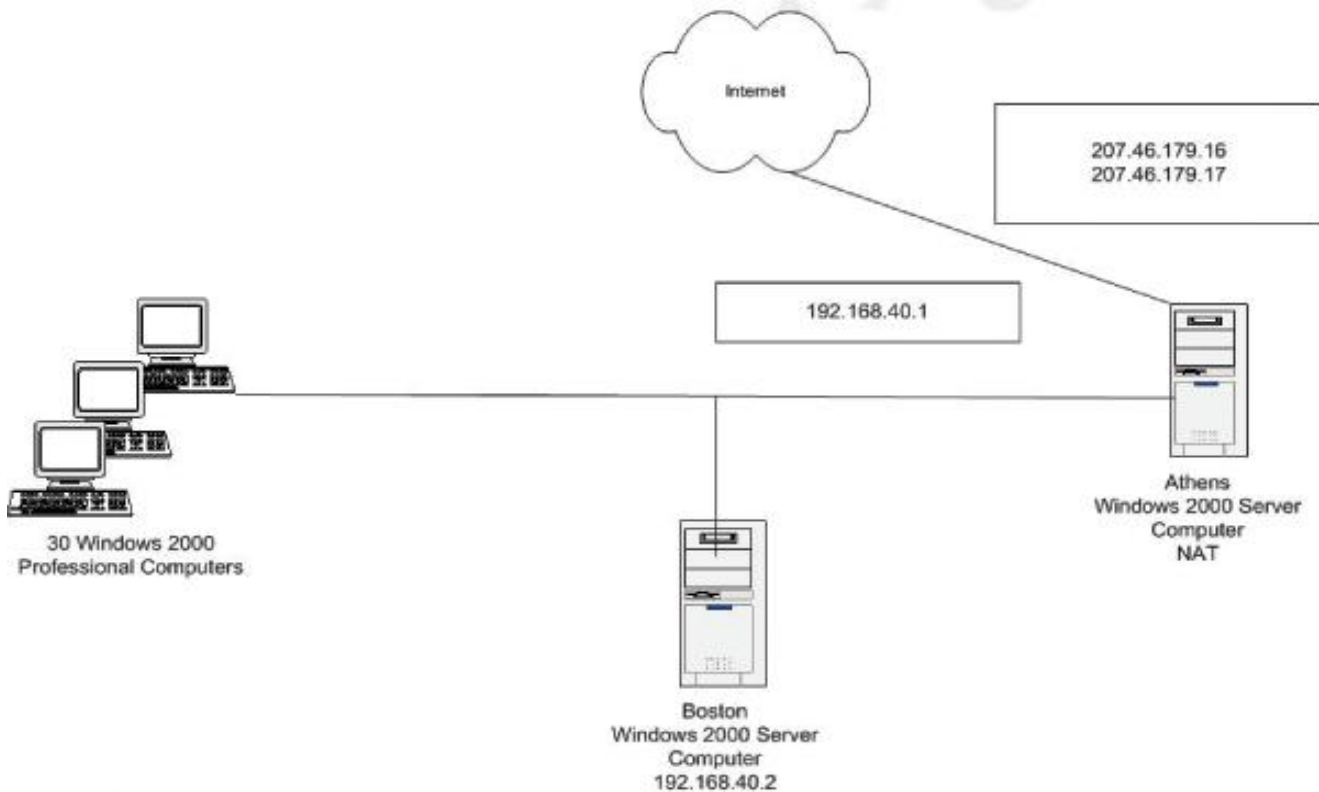
**QUESTION NO: 1**

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:**

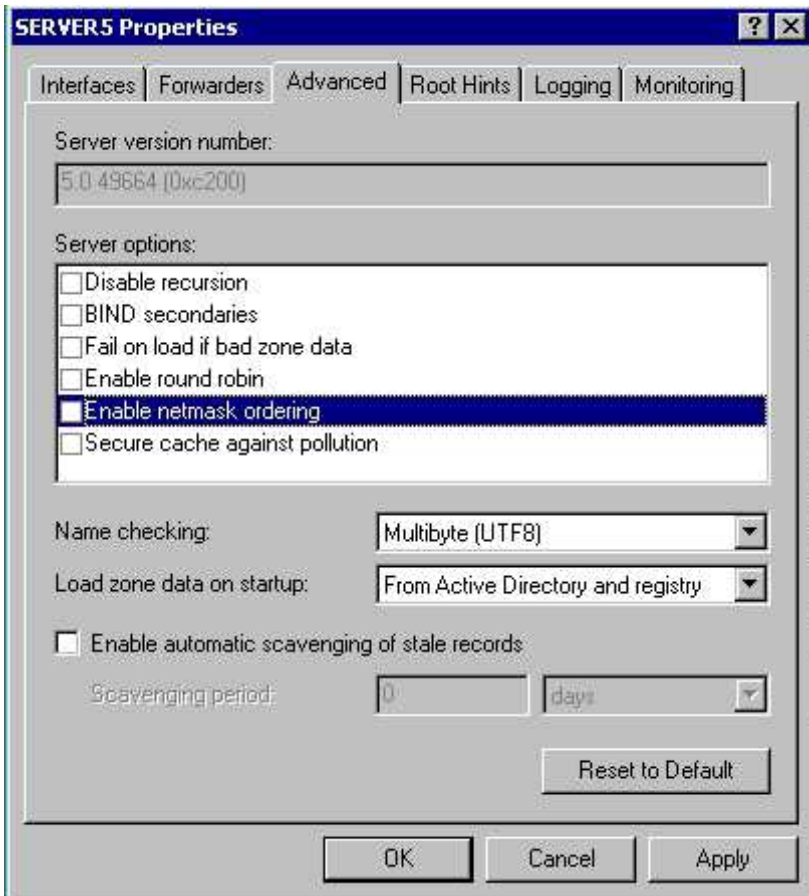
- A:** The demand-dial interface must be put on the dial-up connection not the local area connection.
- D:** On the private interface the default gateway (from the clients point of view) is the NAT computer.
- G:** The address pool consists of public addresses. The ISP provides 1 or more public IP addresses. 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 Chinatag'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 Chinatag'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 Chinatag'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 Chinatag'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 member 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.

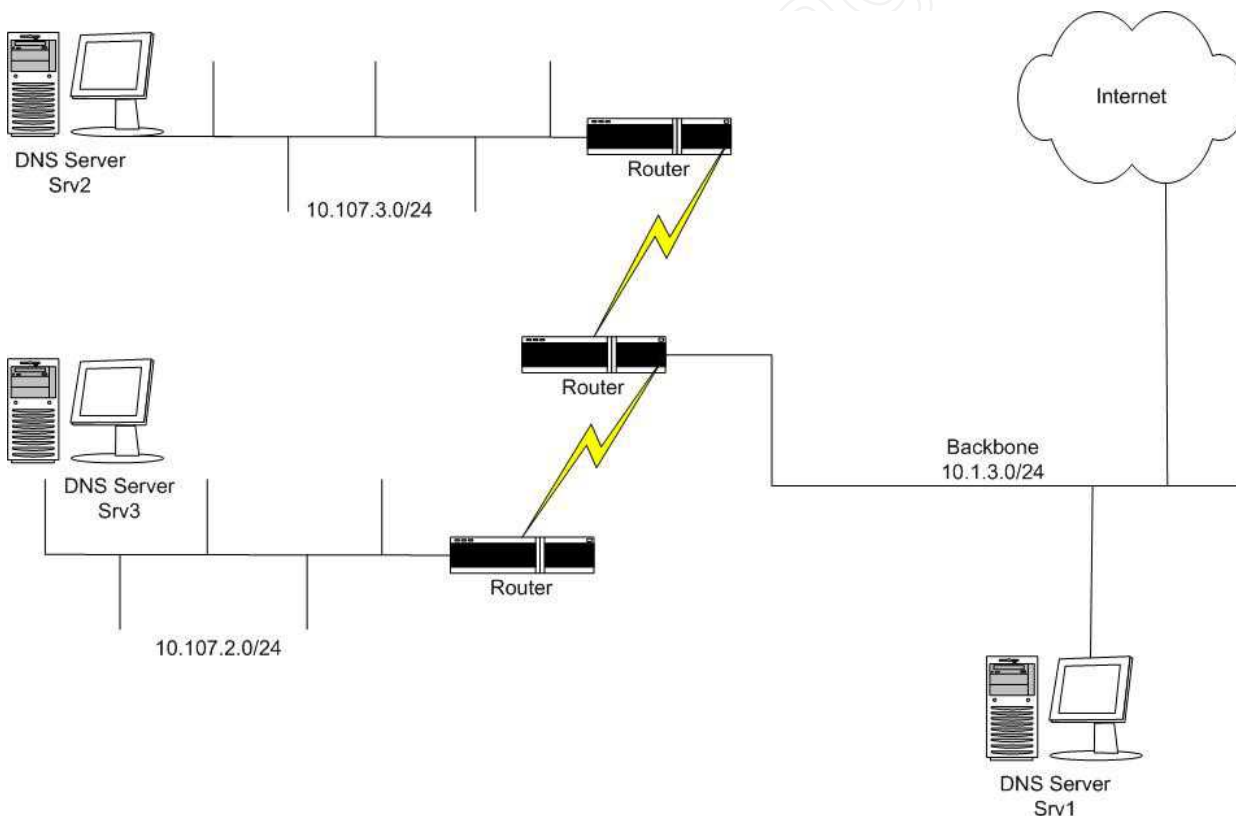
This reduces network traffic across subnets by forcing computers to connect to network resources that are closer to them.

**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.**

**Your 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 Chinatag’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 Chinatag'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.
- Rogue 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. 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 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.**