CHAPTER THREE

3 Managing Name Resolution

Terms you'll need to understand:

- ✓ Windows Internet Naming Service (WINS)
- ✓ WINS Proxy Agent
- ✓ LMHOSTS
- ✓ Tombstoning
- ✓ Persistent Connections
- ✓ Push/pull partner
- ✓ Hostnames
- ✓ Domain name system (DNS)
- ✓ Recursive and iterative queries
- ✓ Primary, secondary, and stub zones
- ✓ Dynamic update
- ✓ Delegation
- ✓ Caching-only server
- ✓ Root name server
- ✓ Resource records

Techniques you'll need to master:

- ✓ Understanding NetBIOS name resolution methods
- ✓ Installing and configuring WINS
- ✓ Configuring a WINS proxy agent
- ✓ Configuring replication between WINS servers
- ✓ Managing and monitoring a WINS server
- ✓ Installing and configuring the DNS Server service
- ✓ Configuring zones
- ✓ Understanding a caching-only server
- ✓ Understanding DNS zone types
- ✓ Managing zones and resource records
- ✓ Implementing a delegated zone for DNS
- ✓ Monitoring a DNS server

Each machine on a computer network is assigned a unique network address. Computers communicate with one another across networks by connecting to these network addresses. These numbers, also known as Internet Protocol (IP) addresses, consist of four groups of numbers, or octets, and can be difficult for people to remember. To solve this dilemma, a system was developed whereby people can use "friendly" names that are then translated automatically into IP addresses that computers use to locate each other and to communicate. These friendly names are called *hostnames*, and each machine is assigned one. Groups of these hosts form a *domain*. The software that translates these names to network addresses is called the *Domain Name System (DNS)*.

Before the advent of DNS, HOSTS files were used for name resolution, but as the Internet quickly grew in size and popularity, HOSTS files became impossible to maintain and keep current. When the Internet community realized there was a need for a more manageable, scalable, and efficient name-resolution system, DNS was created. Since that time, DNS servers have been used on the Internet almost exclusively.

Before the introduction of Windows 2000, Network Basic Input/Output System (NetBIOS) names were used to identify computers, services, and other resources on Windows-based machines. In the early days of Windows networks, LMHOSTS files were used for NetBIOS name resolution. Later, these names were often resolved to IP addresses using a NetBIOS Name Server (NBNS). Microsoft's version of the NBNS was called Windows Internet Naming Service (WINS). With Windows 2000 and Windows Server 2003, hostnames are used instead of NetBIOS names. In a Windows Server 2003 domain, DNS is used to resolve hostnames and locate resources such as network services.

This chapter introduces the Windows Server 2003 implementation of WINS and DNS. You'll learn how to install and configure both name resolution services, as well as how to maintain and monitor them. Having a thorough understanding of the topics presented here is important to both the exam and on-the-job success.

Introduction to NetBIOS Name Resolution

Some clients still rely on NetBIOS names to communicate with other hosts on a network. A NetBIOS name is a 16-character name where the first 15 characters identify a unique host and the 16th character identifies a service or application running on the host such as the Workstation or Server service. Table 3.1 outlines common hexadecimal values used to identify services running on a computer.

TABLE 3.1 Node Types

Node Type	Description
<00H>	Registered by the Workstation service
<1CH>	Indicates a domain name that can be used to locate domain controllers
<06H>	Registered by a computer running Routing and Remote Access
<1BH>	Registered by each domain controller functioning as the domain master browser
<20H>	Registered by a WINS client running the Server service
<21H>	Registered by the RAS client running on a WINS client

As with domain names, NetBIOS names must be resolved to an IP address before two hosts can communicate. There are a number of different methods available for name resolution and the method employed will depend on the environment.

Name Resolution Methods

The three standard ways of resolving NetBIOS names to IP addresses are through a local broadcast, using the local cache, or by using a NetBIOS name server.

With a local broadcast, a broadcast is sent out on the network requesting the IP address of a specific host. The obvious disadvantage to this method is the increase in traffic.

All hosts maintain a local cache that can be used for name resolution. Each time a host resolves a NetBIOS name to an IP address, the record is added to the local cache and remains valid for 10 minutes. By default, all clients will check their local cache before using any of the other resolution methods available.

The third option is to use a NetBIOS name server (such as a WINS server) to resolve names to IP addresses.

In a Microsoft environment, several other methods for resolving names are also available such as DNS servers, HOSTS files, and LMHOSTS files.

Depending on the requirements of an environment, clients can be configured to use a single method for name resolution or they can use a combination of methods. The exact method a client uses to resolve NetBIOS names is determined by their node type. For example, if a client is configured as an M-Node, it will attempt to resolve a NetBIOS name by first performing a local broadcast. If this is unsuccessful, it will then try to resolve the name using a NetBIOS name server. You can check the node type a client is configured for by typing **`ipconfig/all`** at the command prompt. The node type can be changed within the local Registry. Table 3.2 summarizes the four different node types.

TIP

Remember that before performing a broadcast or contacting a WINS server, the host will attempt to resolve a NetBIOS name using its local cache.

EXAM ALERT

Be prepared to encounter exam questions pertaining to the NetBIOS node types. Make sure you are familiar with what methods of resolution are used for each type and in what order.

TABLE 3.2 Node Types

Node Type	Description
B-Node	A broadcast is used for NetBIOS name registration and resolution.
P-Node	A NetBIOS name server is used for name registration and resolution.
M-Node	A broadcast is attempted first for name resolution. If this method fails, a NetBIOS name server is contacted.
H-Node	A NetBIOS name server is attempted first for name resolution. If this fails a broadcast is used.

EXAM ALERT

A Windows Server 2003 or Windows XP client that is configured as a DHCP client automatically uses H-Node for NetBIOS name resolution. This means the client will attempt to resolve NetBIOS names using a WINS server first before using a local broadcast (after checking the local cache). The client will resolve names in the following order: local cache, WINS, broadcast, LMHOSTS, HOSTS, DNS.

LMHOSTS Files

As already mentioned, one of the ways in which NetBIOS names can be resolved is through the use of a text file known as an LMHOSTS file. One of the benefits of using an LMHOSTS file is that entries from the file can be preloaded into the local cache to facilitate name resolution (because this is the method a client will use to resolve a NetBIOS name). So if a client cannot resolve a NetBIOS name using any of the methods described previously, it can parse the LMHOSTS file to see whether a record exists.

TIP

Remember that in order for clients to resolve names using an LMHOSTS file, they must be configured to do so (refer to the section "Configuring WINS Clients" for more information).

The LMHOSTS file can be found in the `%systemroot%\system32\drivers\etc` directory. When configuring records within the file, there are several directives that can be used which are outlined in Table 3.3.

TABLE 3.3 Predefined Directives That Can Be Used Within an LMHOSTS File

Predefined Keyword	Description
`#Pre`	Defines which entries within the file should be loaded into the local cache.
`#DOM:`*`domain_name`*	Indicates the record is for a domain controller.
`#Begin_Alternate`	Specifies a list of other locations for an LMHOSTS file.
`#End_Alternate`	
`#inlcude`	Loads entries from a separate LMHOSTS file separate from the default file on the local computer. This option is most often used to specify a centrally located LMHOSTS file.
`#MH`	Adds multiple entries for a multihomed computer.

EXAM ALERT

Be sure you are familiar with the different directives that can be used within an LMHOSTS file and what their purposes are.

Introduction to WINS

The Windows Internet Naming Service (WINS) provides a dynamic database to register NetBIOS names and resolve them to IP addresses. Clients can dynamically register their NetBIOS names with a WINS server, and query the WINS server when they need to resolve a NetBIOS name to an IP address.

WINS solves the problem of registering and resolving NetBIOS names in a routed environment. In a nonrouted environment, NetBIOS names can be registered and resolved using local broadcasts. However, in a routed environment this poses a problem because routers are not normally configured to forward broadcasts between subnets.

By using WINS, name registration and renewal requests can be directed to a WINS server, thereby allowing name registration and renewal across subnets.

There are a number of other benefits to implementing a WINS server on the network including the following:

- It provides a dynamic database for registering NetBIOS names and resolving them to an IP address.
- It centralizes the management of NetBIOS names to IP addresses and eliminates the need for LMHOSTS files.
- It reduces the amount of broadcast traffic on the network. Clients can directly query the WINS server for name registration and resolution instead of performing a broadcast.
- It allows pre–Windows Server 2003 clients to locate domain controllers that are not on their local subnet.

Installing WINS

WINS is not a service that is installed by default. It can be added afterward through the Add or Remove Programs applet in the Control Panel.

To install WINS:

1. Point to Start, Settings, and click Control Panel.
2. Double-click the Add or Remove Programs applet. Click Add/Remove Windows Components.
3. In the list of components, select Networking Services and click Details.
4. Click Windows Internet Name Service (WINS) and click OK.

Configuring a WINS Server

You can configure and manage a WINS server through the WINS management console. Click Start, Administrative Tools, and then WINS.

Within the WINS console, right-click the WINS server and click Properties. You can configure several options from the Properties dialog box.

Using the General tab, you can configure how often server statistics are updated (you can also disable this option) and specify a location to back up the WINS database.

From the Intervals tab, the rate at which records are renewed, deleted, and verified can be configured (see Figure 3.1). Table 3.4 summarizes the configurable options.

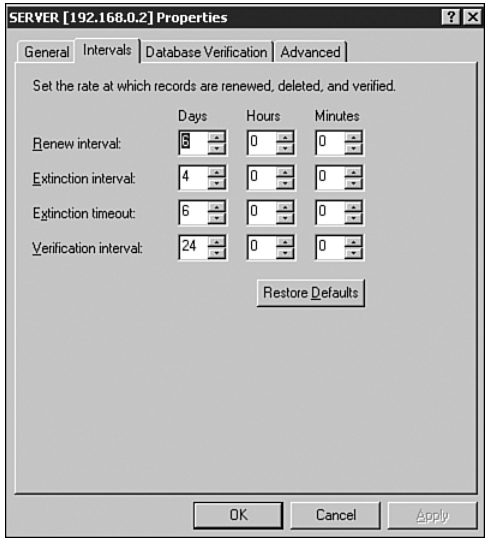


FIGURE 3.1 Configuring the rate at which records are renewed, deleted, and verified.

TABLE 3.4 Zone Property Tabs

Option	Description
Renew Interval	Specifies the number of days before a WINS client must renew its registered NetBIOS name.
Extinction Interval	Specifies the amount of time before a record marked as released is marked as extinct.
Extinction Timeout	Specifies the amount of time before a record marked as extinct is removed from the WINS database.
Verification Interval	Specifies the amount of time before a WINS server must verify any records that have been replicated from a replication partner.

NOTE

The process of deleting records marked as extinct is known as scavenging. Using the Scavenge Database option allows an administrator to manually initiate the scavenging process.

The Database Verification tab enables you to configure when and how often the WINS server should verify the records within its database.

The Advanced tab has several configurable options (see Figure 3.2). You can enable logging so WINS-related events are written to the System Log. Burst Handling can be enabled or disabled, which enables you to configure the number of requests a WINS server can successfully respond to without actually

registering the name within the database. You can also specify the location of the WINS database and configure the version number.

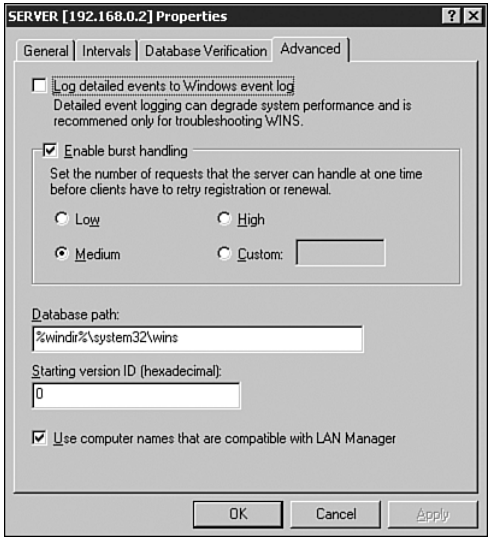


FIGURE 3.2 Configuring Advanced server options.

TIP

Making configuration changes to any server can have negative effects. A user can be permitted to view the contents of the WINS database while not being able to make configuration changes by adding the user account to the WINS Users group.

WINS Replication

Consider the following scenario: Two subnets exist on a physical network each with its own WINS server. Clients on each subnet register their names with their local WINS server. When a host on subnet A attempts to communicate with a host on subnet B, they will be unable to resolve the name to an IP address. This is due to the fact that the local WINS server will not have an entry in its database for the host on subnet B.

In a WINS environment, replication must be configured between WINS servers to facilitate network communication between hosts on different subnets. WINS servers can be configured as push partners, pull partners, or both depending on how you want replication to occur.

Push partners notify other WINS servers when changes are made to its database, whereas pull partners request database changes from other WINS servers. In order to accomplish one-way replication one of these partnerships (either a push or pull) must be configured.

When considering whether to configure push or pull partners, keep the following points in mind:

- If WINS servers are connected by slow links, configure a pull partner so replication can be scheduled.
- If WINS servers are connected by fast links, configure a push partner so replication can occur when changes are made to the database.

Configuring WINS Replication

WINS servers can be configured for replication using the WINS management console. To configure replication, follow these steps:

1. Within the WINS management console, right-click Replication Partners and select New Replication Partner.
2. Enter the name or IP address of the WINS server you want to add as a replication partner. Click OK.
3. Right-click the WINS server that was added as a replication partner and click Properties.
4. From the Advanced tab within the WINS server's properties window, use the drop-down list to select the replication partner type. Click OK.

If you do not want to manually set up WINS replication partners, you can configure WINS servers to automatically find one another and configure themselves for replication. They do so by multicasting to the IP address of 224.0.1.24. When WINS servers locate each other they automatically configure themselves as push/pull replication partners. This automatic discovery option can be enabled by right-clicking Replication Partners within the WINS management console and clicking Properties. From the Replication Partners Properties window, select the Advanced tab and choose the Enable Automatic Partner Configuration option.

Forcing Replication

The replication of WINS records between WINS servers normally occurs in any of the following situations:

- When a WINS server starts up

- When the number of changes to the database reaches a certain number
- At specific intervals configured by an administrator

Sometimes, however, you may need to update the WINS database immediately. Within the WINS management console, administrators have the option of forcing replication to occur between WINS partners. To force replication between replication partners, click Replication Partners, right-click the server you want to replicate with, and select either Start Push Replication or Start Pull Replication.

Persistent Connections

One of the features introduced in Windows 2000 and supported by Windows Server 2003 is persistent connections between WINS replication partners. In previous versions of Windows, WINS servers disconnected from one another when replication was complete. Each time the replication process occurred, a new connection needed to be established requiring more processor cycles. In other words, it's inefficient, especially if the WINS servers are connected with high-speed links. To make the replication process more efficient, administrators could configure replication to occur after a large number of changes occurred to the database, as opposed to having to reestablish a connection for a small number of changes. In any case, replication was slow and it was not uncommon to find inconsistencies in the WINS database.

With persistent connections, WINS servers no longer close connections after replication is complete. Not only does this increase the speed and efficiency of replication, as changes can be sent without having to wait for a connection to be established, but it also makes for more consistency within the WINS database.

Managing and Monitoring WINS

Most management and monitoring tasks can be performed within the WINS management console. Most of the maintenance tasks performed will be to the WINS database, such as ensuring it is backed up in the event it becomes corrupt, and ensuring the database remains consistent over a period of time.

Backing Up and Restoring the WINS Database

Through the WINS management console, you can configure a WINS server to periodically back up its local database. From the WINS server properties window,

you can specify a backup location. You can also right-click the WINS server and select the Backup database option.

After you specify a backup location the WINS server will create the `Wins_bak\NewFolder` within the location you specify and back up the local database to this location every three hours. You also have the option of selecting whether the WINS server should perform a backup when the server is shut down.

If you have a backup of the WINS database, you can restore it by right-clicking the WINS server, choosing the Restore Database option, and specifying the location of folder where the database was backed up to. Keep in mind that before you perform a restore, the WINS service must be stopped. If the WINS service is running, the option to restore the database will not be available.

Server Statistics

Viewing the statistics of a WINS server can provide an administrator with a general idea of what is happening. Within the WINS management console, you can right-click the WINS server and select the Display Server Statistics option. Some of the information provided includes when the server was last started, when replication last took place, and the number of name queries resolved.

Tombstoning

Records that are deleted or marked as extinct on one server can cause inconsistencies to the database of its replication partners. For example, a record that was deleted from the database on one server can easily still appear within the database of a replication partner.

Windows Server 2003 supports a feature known as tombstoning. After a record is marked as tombstoned it is no longer considered to be active on the local WINS server. The record remains within the local database for replication purposes. When a tombstoned record is replicated, all replication partners mark the record as being tombstoned and it becomes extinct, eventually being removed from the database.

Records within the WINS database can be manually deleted or tombstoned using the following process:

1. Within the WINS console, right-click the Active Registrations container and click either the Find by Name or Find by Owner option to locate the appropriate record.
2. If you select Find by Name, type in the NetBIOS name you are searching for. If you select Find by Owner, specify whether to have all entries

in the local WINS database displayed or records from a specific WINS server. Click Find Now.

3. In the Details pane right-click the appropriate record and click Delete.
4. Within the Delete Record dialog box select one of the following options: Delete the Record Only from this Server or Replicate Deletion of the Record to Other Servers (Tombstone).

Verifying Database Consistency

With multiple WINS servers configured for replication, a WINS database can become inconsistent over a period of time. Using the Verify Database Consistency and Verify Version ID Consistency options, an administrator can periodically perform database consistency checks. Checking the WINS database for inconsistencies will force the local WINS server to check all names replicated from other WINS servers and compare them with the local versions on the servers that own the records. The WINS server will then update its local records.

Configuring WINS Clients

In order for clients to dynamically register their NetBIOS names with a WINS server and use the server for name resolution, they must be configured with the IP address of the WINS server. A WINS client can be running any of the following platforms:

- Windows Server 2003
- Windows XP
- Windows 2000
- Windows NT 3.51 and later
- Windows 95
- Windows 98
- Windows for Workgroups 3.11 running MS TCP/IP32
- Microsoft Network Client 3.0 for MS-DOS
- LAN Manager 2.2c for MS-DOS

There are two methods available for configuring clients with the IP address of the WINS server. You can use a DHCP server or you can configure each client manually.

If you opt to use DHCP, clients will require no configuration as they are enabled for DHCP by default. But you will have to configure the DHCP server to assign the IP Address of the WINS server to DHCP clients. To do so, configure the 044 WINS/NBNS server and the 046 WINS/NBT Node type DHCP options. You can do so by configuring the scope options within the DHCP management console (refer to Chapter 2, "Managing IP Addressing," for instructions on how to configure scope options).

The first option specifies the IP address of the WINS server. The second option specifies the node type or methods clients use to resolve NetBIOS names and in what order.

Clients can also be configured manually by an administrator, which means visiting each workstation and typing in the IP address of the WINS server. To manually configure a Windows XP client for WINS, follow these steps:

1. Point to Start, Settings, and click Network Connections.
2. Right-click the Local Area Connection and click Properties.
3. From the list of components select Internet Protocol (TCP/IP) and click Properties.
4. From the Internet Protocol (TCP/IP) Properties window, select the Advanced button and click the WINS tab.
5. Click the Add button and type in the IP address for the WINS server. Repeat the process for additional WINS servers on the network. Click OK.

There are several other configurable options available on the WINS tab, which are summarized as follows:

- *Enable LMHOSTS Lookup*—This option is selected by default and it enables the client to use an LMHOSTS file to resolve NetBIOS names to IP addresses. The Import LMHOSTS button allows you to import an existing file into the LMHOSTS file on the client computer.
- *Enable NetBIOS over TCP/IP*—This option specifies that the local area connection uses NetBIOS over TCP/IP and WINS. This setting should be enabled if the computer must communicate using computer names or with pre–Windows 2000 clients.
- *Disable NetBIOS over TCP/IP*—This option disables NetBIOS over TCP/IP and WINS for the local area connection. On a network that runs only Windows 2000, this option can be selected.

- *Use NetBIOS Setting from the DHCP Server*—Select this option to have the client obtain WINS information from a DHCP server. If the client is configured to receive its IP address from a DHCP server, this option is selected by default.

Configuring Static Mappings

In some cases there may be clients on the network that are unable to dynamically update their NetBIOS name with a WINS server. In these instances, a static mapping can be manually added to the WINS database by an administrator. After a static mapping is created, it does not need to be renewed, nor does it expire. The entry must be manually deleted by an administrator.

To configure a static mapping:

1. Click Start, point to Programs, Administrative Tools, and click WINS.
2. Within the WINS management console, right-click Active Registrations and select New Static Mapping.
3. In the New Static Mapping dialog box, type in the computer name (NetBIOS name) for the host.
4. If required, type in the NetBIOS scope.
5. Using the drop-down arrow, select the type of entry you are creating.
6. Type in the IP address of the host. Click OK.

Keep in mind that if the client for which you created a static mapping is also a DHCP client, a client reservation should be created for it so it is leasing the same IP address all the time. If the client leases an IP address different from the IP address listed in the WINS database, the name will be resolved to the incorrect IP address.

WINS Proxy

Clients that do not support WINS may resolve NetBIOS names using a broadcast. For routed IP networks, this method of name resolution becomes difficult if not impossible all together. In these situations, you can configure what is known as a WINS proxy agent.

A *WINS proxy* is a computer on a local subnet that listens for name resolution broadcasts. After the WINS server receives a broadcast, it queries the WINS server on behalf of the non-WINS client and returns the results. In terms of

NetBIOS name registration, the WINS proxy also listens for name registration broadcasts on the local subnet. When a non-WINS client attempts to register its NetBIOS name, the WINS proxy queries the WINS server to ensure that the name has not already been registered by another host.

To configure a computer to act as a WINS proxy, you must edit the local Registry. To do so, navigate to `HKEY_LOCAL_MACHINE\system\currentcontrolset\services\netbt\parameters` and change the value for the EnableProxy to 1.

DNS Concepts

At one time or another, most of us have typed a universal resource locator (URL) to get to one of our favorite websites. Before you can view the website stored on a web server, that URL you typed must be resolved to an IP address, and this is where DNS servers come into play.

You might have also heard the term *fully qualified domain name (FQDN)*. An FQDN contains both the hostname and a domain name. It uniquely identifies a host within a DNS hierarchy. For example, www.bayside.net is an FQDN. Every FQDN is broken down into different levels, each separated by a period. In the preceding example, .net is the top-level domain and bayside is the second-level domain. The top-level domain normally identifies the type of organization, such as a government organization (gov) or an educational organization (edu). The second-level domain indicates a specific domain within that top-level namespace, whereas the third level might indicate a specific host within that domain. In all cases, DNS servers are used to resolve FQDNs to IP addresses.

DNS Queries

A DNS query is a request for name resolution. Name resolution requests can be initiated by both DNS clients and DNS servers. A DNS client sends a query to a DNS server and a DNS server can send a query to another DNS server on behalf of a client.

DNS can use two different processes to resolve queries: recursive and iterative. With a *recursive query*, the DNS client requires the DNS server to respond with the IP address of the request or an error message that the requested name does not exist. The DNS server cannot refer the client to another DNS server if it cannot map the request to an IP address. When a DNS server receives a recursive request, it queries other DNS servers until it finds the information or until the query fails.

With an *iterative query*, the DNS server uses zone information and its cache to return the best possible answer to the client. If the DNS server does not have

the requested information, it can refer the client to another DNS server. An iterative query is typically performed by a DNS server once it has received a recursive query from a DNS client.

For example, when a DNS client enters www.bayside.net into a browser, the following process occurs:

1. A DNS client sends a recursive query to the local DNS server.
2. Before forwarding the request to a root server, the DNS server checks its local cache to determine whether the name has recently been resolved. If there is an entry in the local cache, the IP address is returned to the client.
3. If no entry exists in the cache for the hostname, an iterative query is sent by the DNS server to a root name server.
4. The *root name server* refers the DNS server to a name server responsible for the first-level domain within the hostname. For example, the root name server would refer the request to the bayside.net DNS server.
5. The original DNS server is referred to second-level DNS servers, and then third-level DNS servers, until one of them can resolve the hostname to an IP address and return the results back to the client.

DNS Forwarders

DNS servers often must communicate with DNS servers outside of the local network. A *forwarder* is an entry that is used when a DNS server receives DNS queries that it cannot resolve locally. It then forwards those requests to external DNS servers for resolution.

By configuring forwarders, you can specify which DNS servers are responsible for handling external traffic. Otherwise, all DNS servers can send queries outside of the local network, possibly exposing DNS information to untrusted hosts on the Internet. Configuring forwarding adds another level of security to the network because only servers identified as forwarders are permitted to forward queries outside the local network.

Additionally, if all DNS servers were allowed to forward queries outside the network, the result could be a large amount of unnecessary network traffic. This can become an important issue if the Internet connection is slow, costly, or already heavily used. Because a forwarder receives queries from local DNS servers, it builds up a large amount of cache information. This means that many of the queries received by the forwarder can be resolved from the cache instead of forwarding the requests outside the local network. This is obviously more efficient in terms of network traffic.

When a DNS server configured to use forwarding receives a DNS query from a DNS client, the following process occurs:

1. The DNS server first attempts to resolve the request using its zone information and information within its local cache.
2. If the request cannot be resolved locally, the DNS server sends a recursive query to the DNS server designated as the forwarder.
3. The forwarder attempts to resolve the query. If the forwarder does not respond, the DNS server attempts to resolve the request by contacting the appropriate DNS server, as specified in the root hints. (Root hints list authoritative root servers for the Internet.)

Conditional Forwarder

A DNS server can be configured to send all queries that it cannot resolve locally to a forwarder, and you can also configure *conditional forwarders*. With conditional forwarders, DNS servers are configured to forward requests to different servers based on the DNS name within the query. When configuring conditional forwarding, you must specify the following information:

- The domain name for which queries will be forwarded
- The IP address of the DNS server for which unresolved queries for a specified domain should be forwarded

EXAM ALERT

You cannot configure a DNS server as a forwarder if a root zone exists. If you plan to configure your DNS server as a forwarder, you must delete the root zone. Open the forward lookup zone in the DNS console. The root zone entry is identified as ".". To delete the root DNS zone, right-click this entry and click Delete.

DNS Server Caching

Caching is designed to improve response times. A DNS server caches the queries that it resolves to improve response time and reduce network traffic.

When performing a recursive query on behalf of a client, the DNS server caches all the information it receives from other DNS servers. Information is kept in the cache for a specified amount of time known as the *Time to Live* (TTL). The TTL is set by the administrator for the primary zone.

When the data is cached, the TTL begins to count down. After the TTL expires, the data is deleted from the cache.

DNS clients also maintain a cache. If a DNS server resolves a query from its cache, it returns the remaining TTL for the data to the DNS client. The DNS client in turn, caches the information and uses the TTL to determine when the entry expires.

Implementing Windows 2003 DNS Server Roles

You can configure a DNS server in one of three possible roles. The role the server plays depends on the configuration of *zone files* and how they are maintained. The zone files contain configuration information for the zone as well as the resource records.

NOTE

A zone file contains the *resource records* for a portion of the DNS namespace. Resource records map hostnames to IP addresses. Both of these topics are covered later in this chapter, in the section "Creating Resource Records."

The three possible DNS server configuration roles are as follows:

- Caching-only server
- Primary server
- Secondary server

Keep in mind when you are planning DNS server roles that a single DNS server can perform multiple roles. For example, a DNS server can be the primary server for one zone and at the same time be a secondary server for another DNS zone.

Caching-Only Server

All DNS servers maintain a `cache.dns` file that contains a list of all Internet root servers. Any time a DNS server resolves a hostname to an IP address, the information is added to the cache file. The next time a DNS client needs to resolve that hostname, the information can be retrieved from the cache instead of the Internet.

Caching-only servers do not contain any zone information, which is the main difference between them and primary and secondary DNS servers. The main purpose of a caching-only server (other than providing name resolution) is to build the cache file as names are resolved. They resolve hostnames, cache the information, and return the results to the client. Because these servers hold no zone

information, either hostnames are resolved from the cache or else another DNS server is required to resolve them.

Caching-only servers are useful when you need to reduce network traffic. Again, because there is no zone information, no zone transfer traffic is generated (meaning that no information is replicated between DNS servers). Hostname traffic is also reduced as the cache file is built up because names can be resolved locally using the contents of the local DNS server's cache.

EXAM ALERT

It's important to understand when caching-only servers should be implemented. Caching-only servers are useful when there are remote locations that have slow WAN links. Configuring a caching-only server in these locations can reduce WAN traffic that would normally be generated between primary and secondary DNS servers, and can speed up hostname resolution after the cache file has been established.

Primary Server

A primary DNS server hosts the working (writable) copy of a zone file. If you need to make changes to the zone file, it must be done from the server that is designated as the primary server for that zone. For those of you who are familiar with Windows NT 4.0, this is similar to how the primary domain controller (PDC) maintains the working copy of the directory database. After a server has been configured as a primary DNS server for a zone, it is said to be authoritative for that domain. Also, a single DNS server can be the primary DNS server for multiple *zones*.

Secondary Server

A secondary server gets all its zone information from a master DNS server. The secondary DNS server hosts a read-only copy of the zone file, which it gets from the primary server or another secondary DNS server. Through a process known as a *zone transfer*, the master DNS server sends a copy of the zone file to the secondary server.

NOTE

Pre–Windows 2000 implementations of DNS supported only full transfers, in which an update to the zone file resulted in the entire zone database being transferred to the secondary servers. Windows Server 2003 (as well as Windows 2000 DNS) supports incremental zone transfers, so the secondary servers can synchronize their zone files by pulling only the changes. This results in less network traffic.

For example, if Server2 is configured as a secondary server for bayside.net, Server2 would get all of its zone information from Server1, the primary DNS server for the zone. Any changes that need to be made to the zone file would have to be done on Server1. The changes would then be copied to Server2. As already mentioned, a DNS server can be both a primary and a secondary server at the same time. Using this example, Server2 could also be configured as the primary server for riverside.net, and, to provide fault tolerance for the zone file, Server1 could be configured as a secondary server for this zone.

Secondary DNS servers provide the following benefits:

- *Fault tolerance*—Because the secondary server has a copy of the zone file, name resolution can continue if the primary DNS server becomes unavailable.
- *Reduction in name-resolution traffic*—Secondary servers can be placed in remote locations with a large number of users. Clients can then resolve hostnames locally instead of having to contact a primary DNS using a WAN link.
- *Load balancing*—Name-resolution services for a zone can be provided by the secondary server as well, thereby reducing the load placed on the primary DNS server.

Installing DNS

DNS can be installed in several ways. It can be added during the installation of Windows Server 2003, after installation using the Configure Your Server Wizard, or through the Add or Remove Program applet in the Control Panel. DNS can also be installed when promoting a server to a domain controller using the `DCPROMO` command.

The only real requirement for installing DNS is Windows Server 2003. It cannot be installed on a computer running Windows XP. Also, if you are using Dynamic Host Configuration Protocol (DHCP) on the network to assign IP addresses, it's generally a good idea to configure the DNS server with a static IP address that is outside the range of addresses included in the DHCP scope.

To install the DNS Server service using the Add or Remove Program applet within the Control Panel, perform the following steps:

1. Click Start, point to Control Panel, and click Add or Remove Programs.
2. Click Add/Remove Windows Components.

3. Highlight Networking Services from the Components list and click the Details button.
4. From the list of components, select Domain Name System (DNS). Click OK and then click Next.
5. After the necessary files are copied, click Finish.
6. Close the Add or Remove Programs applet.

Configuring DNS Server Options

When DNS is installed, the DNS management console is added to the Administrative Tools menu. From the management console, you can manage all aspects of a DNS server, from configuring zones to performing management tasks.

A number of options can be configured for a DNS server. By right-clicking the DNS server within the management console and selecting the Properties option, the properties window for the server is displayed (see Figure 3.3).

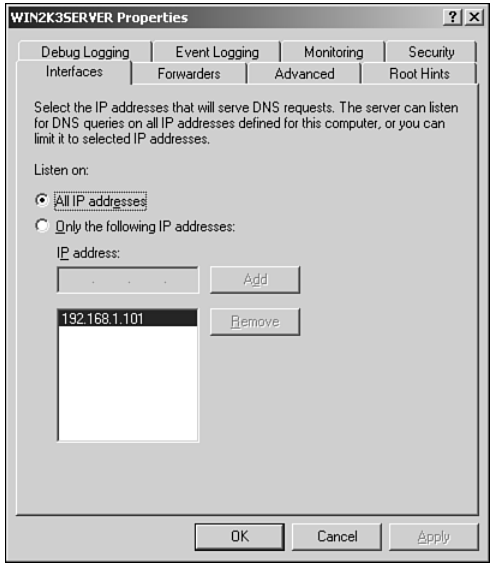


FIGURE 3.3 After installing the DNS service, you can configure DNS server options through the server's Properties dialog box.

The available tabs from the DNS server Properties sheet and their uses are summarized as follows:

- *Interfaces*—Using this tab, you can configure the interfaces on which the DNS server will listen for DNS queries.

- *Forwarders*—From this tab, you can configure where a DNS server can forward DNS queries that it cannot resolve.
- *Advanced*—This tab allows you to configure advanced options, determine the method of name checking, determine the location from which zone data is loaded, and enable automatic scavenging of stale records.
- *Root Hints*—This tab enables you to configure root name servers that the DNS server can use and refer to when resolving queries.
- *Debug Logging*—From this property tab, you can enable debugging. When this option is enabled, packets sent and received by the DNS server are recorded in a log file. You can also configure the type of information to record in the file.
- *Event Logging*—The Event Logging tab enables you to configure the type of events that should be written to the DNS event log. You can log errors, warnings, and all events. You can also turn off logging by selecting No Events.
- *Monitoring*—The Monitoring tab can be used to test and verify the configuration by manually sending queries against the server. You can perform a simple query that uses the DNS client on the local server to query the DNS service to return the best possible answer. You can also perform a recursive query in which the local DNS server can query other DNS servers to resolve the query.
- *Security*—This tab enables you to assign permissions to users and groups for the DNS server.

EXAM ALERT

Windows Server 2003 DNS supports fast zone transfers. This feature is not supported by DNS servers running BIND versions older than 4.9.4. This feature must be enabled on the Advanced tab to support zone transfers with DNS servers running older versions of BIND.

Advanced DNS Server Options

There are several options that can be configured using the Advanced tab of the DNS server's properties window. Generally, the default settings should be acceptable and require no modifications. The advanced settings that can be configured are summarized in the following list:

- *Disable Recursion*—This determines whether the DNS server uses recursion. If recursion is disabled, the DNS server will always use referrals, regardless of the type of request from clients.

- *BIND Secondaries*—This determines whether fast transfers are used when transferring zone data to a BIND server. Versions of BIND earlier than 4.9.4 do not support fast zone transfers.
- *Fail on Load if Bad Zone Data*—This option determines whether the DNS server continues to load a zone if the zone data is determined to have errors. By default, the DNS server will continue to load the zone.
- *Enable Round Robin*—This option determines whether the DNS server will rotate and reorder a list of resource records when multiple resource records exist for a query answer.
- *Enable Netmask Ordering*—This determines whether the DNS server reorders host (A) records within the same resource record set in response to a query based on the IP address of the source query.
- *Secure Cache Against Pollution*—This determines whether the DNS server attempts to clean up responses to avoid cache pollution. This option is enabled by default.

Configuring DNS Zone Options

After you have installed the DNS Server service, your next step is to create and configure zones (unless the DNS server is not authoritative for any zones).

A *zone* is basically an administrative entity. A zone is nothing more than a portion of the DNS database that is administered as a single unit. A zone can contain a single domain or span multiple domains. The DNS server that is authoritative for a zone is ultimately responsible for resolving any requests for that particular zone. The zone file maintains all the configuration information for the zone and contains the resource records for the domains in the zone.

Each new zone consists of a forward lookup zone and an optional reverse lookup zone. A *forward lookup zone* maps hostnames to IP addresses. When a client needs the IP address for a hostname, the information is retrieved from the forward lookup zone. A *reverse lookup zone* does the opposite. It allows for reverse queries, or mapping of an IP address back to a hostname. Reverse queries are often used when troubleshooting with the `NSLookup` command.

Zone Types

Windows Server 2003 supports four types of zones:

- *Standard primary zone*—This type of zone maintains the master writable copy of the zone in a text file. An update to the zone must be performed from the primary zone.

- *Standard secondary zone*—This zone type stores a copy of an existing zone in a read-only text file. To create a secondary zone, the primary zone must already exist, and you must specify a master name server. This is the server from which the zone information is copied.
- *Active Directory–integrated zone*—This zone type stores zone information within Active Directory. This enables you to take advantage of additional features, such as secure *dynamic updates* and replication. Active Directory–integrated zones can be configured on Windows Server 2003 domain controllers running DNS. Each domain controller maintains a writable copy of the zone information, which is stored in the Active Directory database.
- *Stub zone*—This type of zone is new in Windows Server 2003. A stub zone maintains only a list of authoritative name servers for a particular zone. The purpose of a stub zone is to ensure that DNS servers hosting a parent zone are aware of authoritative DNS servers for its child zones. One of the advantages of stub zones is that they create a dynamic relationship between the parent and child. Compared to delegation, which points to a single IP address, stub zones allow much more flexibility for the administrator because changes in the child zone are automatically reflected in the stub without making changes to the configuration.

Stub Zones Versus Conditional Forwarding

A *stub zone* is an actual zone that would exist on the DNS server that contains just the SOA record for the zone it refers to and the DNS server's records and glue records (host A records). The stub zone replicates from the master DNS server in the zone it refers to and will keep current with DNS servers for that zone/domain. It is more work to set up than conditional forwarding and requires permission from the administrator of the other domain because it does zone transfers with it. However, it is more reliable in keeping current with the DNS servers in the zone.

Stub zones provide a way for DNS servers hosting a parent zone to maintain a current list of the authoritative DNS servers for the child zones. As authoritative DNS servers are added and removed, the list is automatically updated.

Conditional forwarding, on the other hand, is used to control where a DNS server forwards queries for a specific domain. A DNS server on one network can be configured to forward queries to a DNS server on another network without having to query DNS servers on the Internet.

EXAM ALERT

Stub zones provide an advantage over conditional forwarding because the information in a stub zone is dynamic, whereas the list of conditional forwards must be updated by a DNS administrator.

Creating Zones

After the DNS service is installed, you can manage it using the DNS management console. From this management console, you can begin configuring a DNS server by creating zones. To create a new zone, follow these steps:

1. Click Start, point to Administrative Tools, and click DNS. This opens the DNS management console.
2. Right-click the DNS server and click New Zone. The New Zone Wizard opens. Click Next.
3. Select the type of zone you want to create: primary zone, secondary zone, or stub zone. You also have the option of storing the zone within Active Directory, if it is available. (The option to store information within Active Directory is available only if Active Directory is installed on the local machine.) Click Next.
4. Select the type of zone you want to create: a forward lookup zone or a reverse lookup zone. Click Next.
5. If you select a forward lookup zone, the Zone Name page appears. Type the name for the zone, such as bayside.net. Click Next.
6. If you selected to create a reverse lookup zone, type the network ID (see Figure 3.4). This is used to create the in-addra.arpa domain, with subdomains named using the network ID of the IP address. DNS uses the reverse lookup zone for performing address-to-name translations. For example, a network ID of 192.168.1 would be translated into 1.168.192.in-addra.arpa. Click Next.
7. In the Zone File screen, select whether to create a new zone file or to use an existing one (see Figure 3.5). This option appears when creating a forward or reverse lookup zone. Click Next.
8. Specify how the DNS zone will receive updates from DNS client computers. Three options are available, as shown in Figure 3.6. If the zone is Active Directory–integrated, you can allow secure updates only. You can allow both nonsecure and secure updates, or you can turn off dynamic

updates so that the resource records must be manually updated. Dynamic updates are covered in more detail later in the chapter in the section "Dynamic Updates."

9. Click Finish.

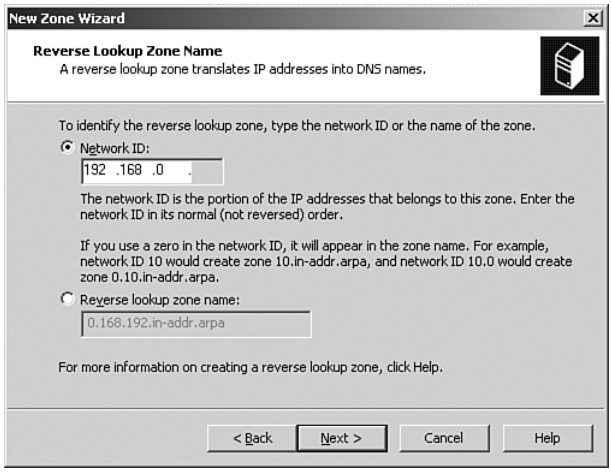


FIGURE 3.4 If you are creating a reverse lookup zone, you must supply the network ID.

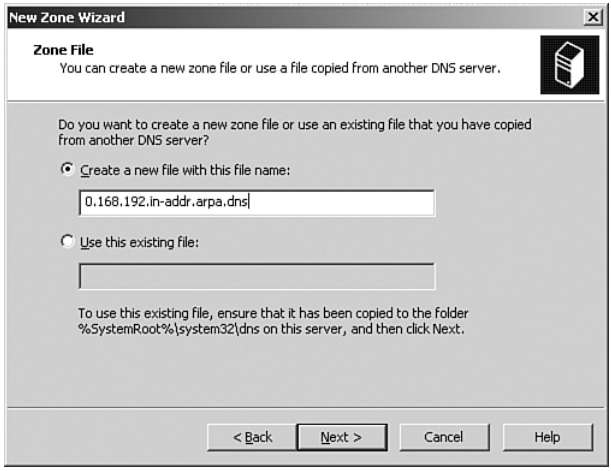


FIGURE 3.5 You must provide a filename for the zone file or select an existing file.

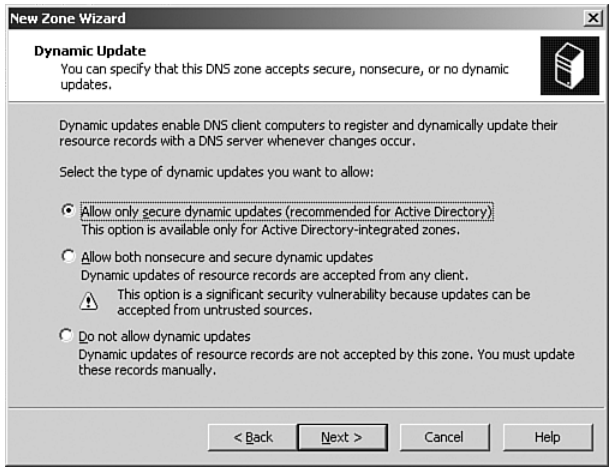


FIGURE 3.6 You must configure how the DNS zone will receive dynamic updates.

Creating Resource Records

After a zone has been created, it can be populated with resource records. Remember, if your clients are all running Windows Server 2003, Windows XP, or Windows 2000 and the zone is configured for dynamic updates, the clients can add and update their own resource records. You can also manually add resource records to a zone file through the DNS management console. A number of resource records can be created. To view all the resource records supported by Windows Server 2003 DNS, right-click a zone and select Other New Records (see Figure 3.7).

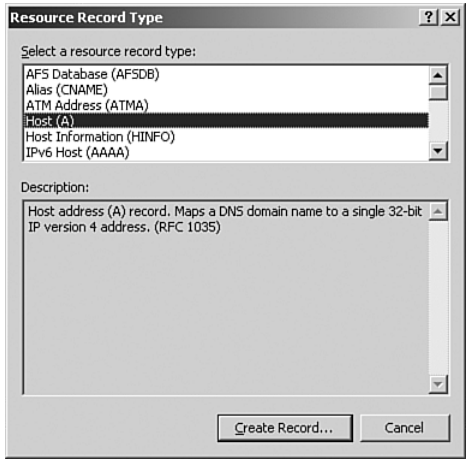


FIGURE 3.7 The next step in zone creation is populating the zone with DNS resource records.

The following list summarizes some of the more common resource records you might encounter:

- *Host Address (A) record*—Maps a DNS name to an IP address. An A record represents a specific device on the network.
- *Start of Authority (SOA) record*—Identifies the primary DNS server for the zone. This is the first resource record in a zone file.
- *Mail Exchanger (MX) record*—Routes messages to a specified mail exchanger for a specified DNS domain name.
- *Pointer (PTR) record*—Points to a location in the DNS namespace. PTR records map an IP address to a DNS name and are commonly used for reverse lookups.
- *Alias (CNAME) record*—Specifies another DNS domain name for a name that is already referenced in another resource record.
- *Service Locator (SRV) record*—Used to identify network services offered by hosts, the port used by the service, and the protocol. SRV records are used to locate domain controllers in an Active Directory domain.

As already mentioned, resource records can be created using the DNS management console. To create a new host record, simply right-click the zone in which you want to create the record and select the New Host (A) option. In the New Host dialog box, type the name and IP address for the host. To automatically create a pointer record, select the Create Associated Pointer (PTR) Record check box (see Figure 3.8).

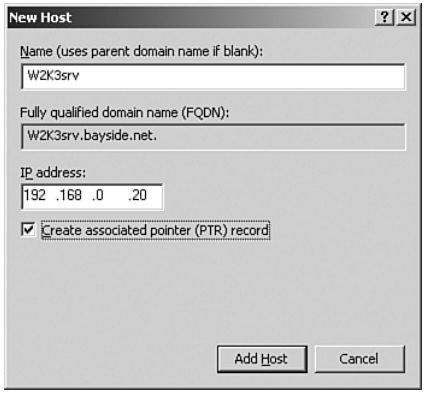


FIGURE 3.8 You can add a new host record via the DNS management console.

To create additional resource records, simply select the type of record you want to create and fill in the required information.

NOTE

The NSLookup command can be used to determine the hostname associated with a specific IP address. To use the NSLookup command, PTR records must exist.

Configuring DNS Simple Forwarding

As you learned earlier in the chapter, a DNS server can be configured to send all queries that it cannot resolve locally to a forwarder. To configure DNS forwarders, follow these steps:

1. Within the DNS management console, right-click the DNS server and click Properties.
2. From the Properties window for the DNS server, click the Forwarders tab.
3. Under DNS Name, select a domain name. To add a new domain name, click the Add button.
4. Under the Selected Domain's Forwarder IP Address list, type the IP address of the forwarder and click Add.

Managing DNS

After DNS is installed, it can be managed using the DNS management console. Management tasks include configuring zone settings, creating and managing resource records, and monitoring the status and performance of DNS. The following sections discuss some of the common management tasks associated with DNS.

Managing DNS Zone Settings

After a zone has been successfully added to your DNS server, you can configure it via the zone's properties dialog box. To do so, right-click the zone from within the DNS management console and click Properties. The Properties dialog box for the zone displays six tabs, as shown in Figure 3.9. If Active Directory is not installed, only five tabs are available (the Security tab is not present).

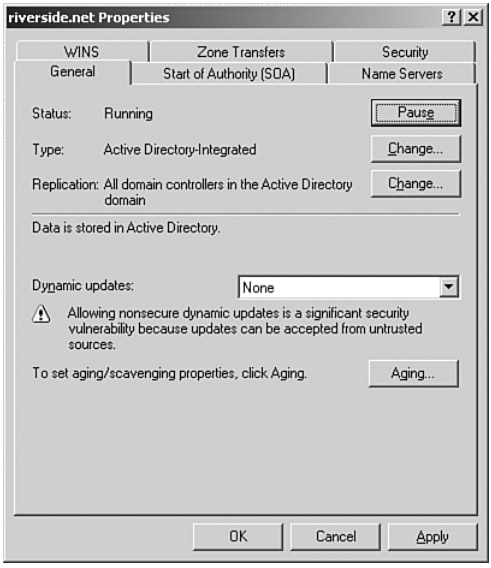


FIGURE 3.9 You can configure a zone through its Properties dialog box.

The following list summarizes each of the tabs for a DNS zone's properties:

- *General*—View the status of the zone, change the type of zone, change the zone filename, change the replication scope for a zone, and configure dynamic updates. You can also set the aging and scavenging properties for the zone.
- *Start of Authority (SOA)*—Configure the zone transfer information and the email address of the zone administrator. The serial number is used to determine whether a zone transfer is required. Each time a change is made this number is incremented by 1. By using the Increment button, you can increase the value, thereby forcing a zone transfer.
- *Name Servers*—Specify the list of secondary servers that should be notified when changes to the zone file occur.
- *WINS*—Enable the DNS server to query the list of WINS servers for name resolution.
- *Zone Transfers*—Configure which secondary servers can receive zone transfers. You can specify any server, only those listed on the Name Servers tab, or the ones configured from this property sheet. Clicking the Notify button enables you to configure which secondary servers will be notified of changes.

- *Security*—If the zone is Active Directory–integrated, the Security tab is available and can be used to configure permissions to the zone file. This is where you can control who can perform dynamic updates.

Changing Zone Types

Using the General tab from the Zone Properties dialog box, you can change the current zone type (see Figure 3.10). To do so, click the Change button beside the zone type. You have the option of changing a primary or secondary zone to an Active Directory–integrated zone or changing an Active Directory–integrated zone to a primary zone or secondary zone.

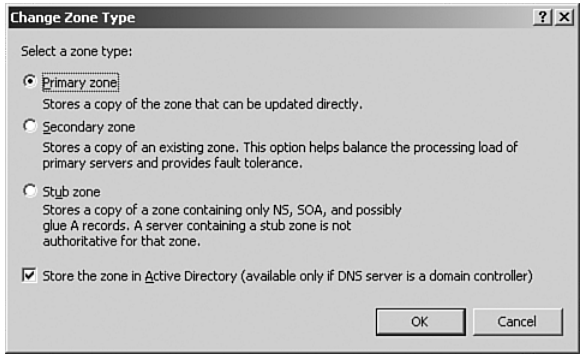


FIGURE 3.10 You can change the zone type via a zone's Properties dialog box.

Before you attempt to change the zone type, be aware of the following points:

- The option to store zone information within Active Directory is available only when the DNS server is also configured as a domain controller.
- If you convert to a secondary zone or a stub zone, you must specify the IP address of the server from which the zone information will be retrieved.
- Changing a secondary zone to a primary zone affects such things as dynamic updates, the use of the DNS Notify option, and zone transfers.
- When the option to store information within Active Directory is cleared, zone information is deleted from Active Directory and copied into a text file on the local DNS server in the `%systemeroot%/system32/DNS` folder.
- Because the purpose of a stub zone is to maintain information about only authoritative name servers for the zone, it is not recommended that a stub zone be converted to a primary zone because primary zones can contain a number of other records rather than just those for authoritative name servers.

Dynamic Updates

Windows 2003 Server, Windows XP, and Windows 2000 clients can interact directly with a DNS server. With dynamic updates, clients can automatically register their own resource records with a DNS server and update them as changes occur. Resource records are the entries within the DNS server database files. Each resource record contains information about a specific machine, such as the IP address or specific network services running. The type of information within a resource record depends upon the type of resource record that is created. For example, an A (address) record contains the IP address associated with a specific computer; it's used to map a hostname to an IP address.

Dynamic updates greatly reduce the administration associated with maintaining resource records. Dynamic updates eliminate the need for administrators to manually update these records. In terms of DHCP, with a short lease duration configured, the IP address assigned to DNS clients can change frequently. If dynamic updates are not enabled, an administrator can end up spending a lot of time updating zone information. In addition, there is always the chance for human error when done manually.

Dynamic updates provide the following advantages:

- DHCP servers can dynamically register records for clients. This is particularly important because DHCP servers can perform updates on behalf of clients that do not support dynamic updates, such as Windows 95, 98, or NT4 clients.
- The administrative overhead is reduced because A records and PTR records can be dynamically updated by Windows DNS clients that support this option.
- The SRV records required to locate domain controllers can be dynamically registered.

EXAM ALERT

To implement dynamic updates on a network with pre–Windows 2000 clients, a DHCP server and a DNS server are required on the network. The DHCP and DNS servers must be running Windows Server 2003 or Windows 2000 because Windows NT 4.0 DNS servers don't support dynamic updates. A DHCP server is required to perform dynamic updates on behalf of clients that do not support this feature, such as Windows 95 clients.

By default, any Windows Server 2003, Windows XP, or Windows 2000 client can update its own records with the DNS server. The DHCP client service

attempts to update records with the DNS server when any of the following events occur:

- The workstation is rebooted.
- The client records are manually refreshed using the `ipconfig /registerDNS` command.
- A statically configured IP address is modified.
- The IP address leased from a DHCP server changes or is renewed. An IP address can be manually renewed using the `ipconfig /renew` option.

Let's take a look at an example of what happens when a Windows XP DNS client performs a dynamic update. Assume that you change a bayside.net workstation's computer name from computer1 to computer2. Upon changing the computer name, you are required to restart before the changes take effect. When the workstation restarts, the following process occurs:

1. The DHCP client service sends a query to an authoritative DNS server for the domain using the new DNS domain name of the workstation.
2. The DNS server that is authoritative for the workstation's domain responds to the request with information about the primary DNS server for the domain.
3. The client sends a dynamic update request to the primary DNS server.
4. The update request is processed by the primary DNS server. The old host and pointer records are removed and replaced with the updated ones.
5. The master name server randomly notifies any secondary servers that a change to the zone file has occurred.
6. Secondary servers request the zone transfer update to the zone file according to the frequency configured on the zone's Start of Authority tab.

Dynamic updates are configured on a per-zone basis. To configure a zone for dynamic update, right-click the zone within the DNS management console and click Properties. In the Properties dialog box, ensure that the General tab is selected. To enable dynamic updates, select one of the following options:

- *None*—Select this option to disable dynamic updates for the zone. Doing this means that the zone file must be manually updated.
- *Nonsecure and Secure*—Select this option to allow nonsecure updates (anyone can perform the update) as well as secure updates (only certain users can perform the update).

- *Secure Only*—Select this option to enable dynamic updates for those users and groups authorized to do so because they have accounts in Active Directory and have been granted permission to update their records. This option is available only for zones that store information within Active Directory. You can use the Security tab from the zone's Properties window to configure who can perform dynamic updates.

EXAM ALERT

When configuring dynamic updates, remember that the zone must be standard primary (information is stored locally in files) or Active Directory–integrated (information is stored on all DCs). Also, to use secure updates, the zone must be Active Directory–integrated. This feature is not supported by standard primary zones.

Secure Updates

Windows Server 2003 supports secure dynamic updates for zones that store information within Active Directory. With secure updates, only those clients authorized within the domain are permitted to update resource records. This means that the DNS server accepts updates only from clients that have accounts within Active Directory. Any computers that do not have accounts are not permitted to register any records, thereby eliminating the chance that unknown computers will register with the DNS server. Secure updates for a zone can be configured by selecting the Secure Only option.

The benefit of selecting this option is obviously an increase in security. The resource records and zone files can be modified only by users who have been authorized to do so. This also provides administrators with a finer granularity of control because they can edit the access control list (ACL) for the zone and specify which users and groups can perform dynamic updates. You edit the ACL for a zone by right-clicking the zone, selecting Properties, and choosing the Security tab.

Zone Transfers

Secondary servers get their zone information from a master name server. The master name server is the source of the zone file; it can be a primary server or another secondary server. If the master name server is a secondary server, it must first get the updated zone file from the primary server. The process of replicating a zone file to a secondary server is referred to as a *zone transfer*. Zone transfers occur between a secondary server and a master name server in the following situations:

- When the master name server notifies the secondary server that changes have been made to the zone file. When the secondary server receives notification, it requests a zone transfer. If multiple secondary servers

exist, they are notified at random so that the master name server is not overburdened with zone transfer requests.

- When the refresh interval expires and the secondary server contacts the primary name server to check for changes to the zone file.
- When the DNS server service is started on a secondary server.
- When a zone transfer is manually initiated through the DNS management console on a secondary server.

Windows Server 2003 DNS (as well as Windows 2000 DNS) supports two types of zone transfers. Pre–Windows 2000 implementations of DNS supported a *full zone transfer (AXFR)* only, in which the entire zone file is replicated to the secondary server. This type of zone transfer is supported by most implementations of DNS. If the secondary server's zone file is not current, which means that changes were made, the entire zone file is replicated. The second type of zone transfer is known as an *incremental zone transfer (IXFR)*, in which only the changes made to a zone file are replicated to the secondary server, thereby reducing the amount of network traffic. Frequency of zone transfers is configured on the Start of Authority tab.

The following list summarizes the configurable options for zone transfers. You can find these options on the SOA tab from the properties window for a zone:

- *Serial Number*—Lists the number used to determine whether the zone file has changed. Each time a change is made, this number is incremented by 1. You can force a zone transfer by manually increasing this number.
- *Primary Server*—Lists the hostname of the primary DNS server for the zone.
- *Responsible Person*—Lists the email address of the person responsible for administering the zone.
- *Refresh Interval*—Determines how often the secondary server polls the primary server for updates. Consider increasing this value for slow network connections.
- *Retry Interval*—Specifies how often the secondary server attempts to contact the primary server if the server does not respond.
- *Expires After*—Specifies when zone file information should expire if the secondary server fails to refresh the information. If a zone expires, zone data is considered to be potentially outdated and is discarded. Secondary master servers do not use zone data from an expired zone.

- *Minimum (Default) TTL*—Specifies how long records from the zone should be cached on other servers.
- *TTL for this Record*—Specifies how long DNS servers are allowed to store a record from the zone in their cache before it expires.

NOTE

When zone information is stored within Active Directory, zone updates are replicated differently than in a standard primary/secondary scenario. DNS notification is no longer needed, and configuring a notify list is unnecessary. Instead, the DNS servers that store information within Active Directory poll Active Directory at 15-minute intervals to check for updates.

Zone Delegation

Delegation is the process of designating a portion of the DNS namespace for another zone. It gives administrators a way of dividing a namespace among multiple zones. For example, an administrator might place the bayside.net domain in one zone and place the sales.bayside.net subdomain in another delegated zone. The bayside.net zone would contain all the records for the sales subdomain if it is not delegated. Through delegating, the bayside.net zone contains only information for bayside.net, as well as records to the authoritative name servers for the sales.bayside.net zone. The host entries for any machines in sales.bayside.net are contained only on the delegated server.

In any case, when deciding whether to delegate, keep the following points in mind:

- Zone delegation allows you to delegate management of part of the DNS namespace to other departments or locations.
- Zone delegation allows you to distribute a large DNS database across multiple servers for load balancing, faster name resolution, and increased performance.
- Zone delegation allows you to extend the namespace for business expansion; that is, it is scalable with business needs.

NOTE

To facilitate the delegation of zones, you need the appropriate delegation records that point to authoritative name servers for the new zone(s).

You can use the following procedure to delegate a zone:

1. From within the DNS management console, right-click the domain you want to delegate and select New Delegation. The New Delegation Wizard opens. Click Next.
2. Type a name for the delegated domain in the Delegated Domain text box. Click Next.
3. Specify the name servers that will host the delegated domain by clicking the Add button. The New Resource Record screen appears, allowing you to specify the name and IP address of the name servers. Click OK. Click Next.
4. Click Finish.

Managing DNS Record Settings

After resource records have been created, they can be managed through the management console. Tasks associated with resource records include modifying the resource records, deleting existing records, and configuring security.

Modifying Resource Records

If you have manually created resource records within a zone, at some point you might need to modify them, such as change the IP address associated with a particular hostname. This won't be an issue if you are using dynamic updates because DNS clients (running the appropriate platform) can update this information on their own.

You can modify a resource record within the DNS management console by selecting the appropriate zone, right-clicking the resource record, and clicking Properties (see Figure 3.11). For example, you can change the hostname, domain name, and IP address of a Host (A) record.

Deleting Resource Records

You can delete resource records within a zone file at any time. For example, if you manually create resource records for a server and remove it from the network, you will want to delete the records from the zone file. Deleting a record is a simple process. Simply right-click the record within the zone and click the Delete option. Click Yes to confirm your actions.

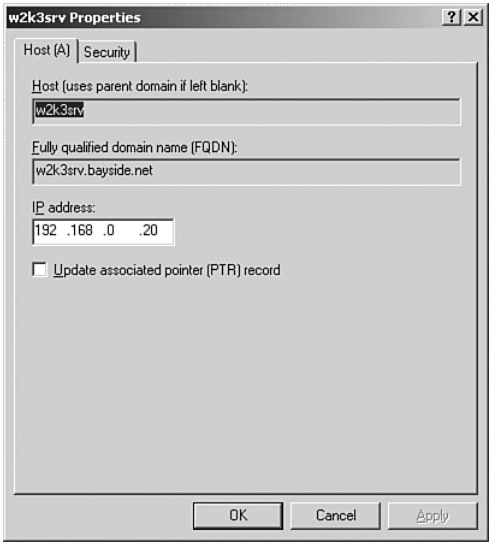


FIGURE 3.11 You can modify the properties of a resource record through the management console.

Modifying Security for Records

Each record has an associated ACL that can be edited. Doing so enables you to specify which users and groups are permitted to securely update the record and change their permissions. You can modify the security by opening the Properties window for a record and selecting the Security tab (see Figure 3.12).

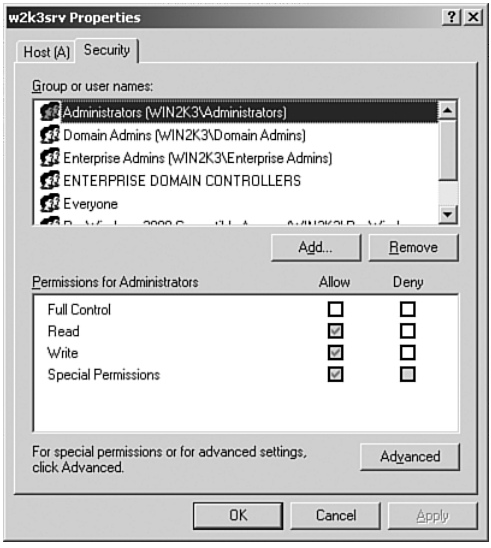


FIGURE 3.12 You modify security for a record on its Security tab.

Managing DNS Server Options

Most management tasks performed on a DNS server are done through the DNS management console. When you highlight your DNS server within the DNS management console and click the Action menu, you see a number of options that can be used to manage different aspects of DNS. Some of the options available are summarized as follows:

- *Set Aging/Scavenging for All Zones*—Use this option to configure refresh intervals for resource records. This enables you to refresh resource records on a set schedule. Refreshing periodically keeps bad records, such as invalid URLs, out of the database.
- *Scavenge Stale Resource Records*—Use this option to manually scavenge stale resource records. Stale resource records can accumulate within a zone over a period of time. For example, if a computer registers its own resource record and is shut down improperly, the record might not be removed from the zone file. Scavenging stale resource records can eliminate any problems, such as outdated information.
- *Update Server Data Files*—Use this option to write all changes to the zone file stored within Active Directory to a zone file on the disk.
- *Clear Cache*—Use this option to clear the contents of the name server's cache.
- *Launch NSLookup*—Use this option to open the command prompt from which you can use the `NSLookup` command.

Monitoring DNS

You should monitor your DNS servers on a regular basis. Obviously, in large enterprise environments, you will want to monitor DNS servers more frequently than for small businesses. Because DNS servers play such an important role for a Windows Server 2003 domain, it's important that solid performance is maintained.

System Monitor

The tool most often used to monitor how services are performing is the System Monitor tool, located within the Performance console. When you install DNS, several counters are added specifically for monitoring this service (see Figure 3.13).

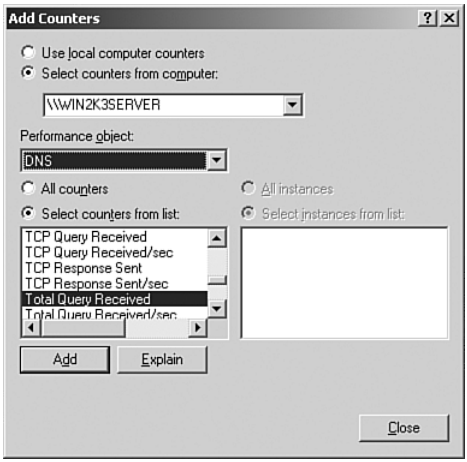


FIGURE 3.13 DNS-specific counters are added to the System Monitor tool for monitoring DNS activity.

The following list outlines some of the common DNS performance counters:

- *Caching Memory*—Monitors the total caching memory used by the DNS server
- *Dynamic Update Received/Sec*—Determines the number of dynamic update requests received by the server per second
- *Dynamic Update Requests*—Counts the total number of dynamic updates received by the server
- *Recursive Queries*—Monitors the total number of recursive queries received by the server
- *Total Queries Received*—Calculates the total number of queries received by the server

Event Viewer

If logging is enabled, DNS-related events can be written to the DNS log. As already mentioned, logging can be enabled using the Event Logging tab from the DNS server's Properties window. By default, all DNS-related events are written to the log. You can choose to log errors only or to log both errors and warnings. By selecting the No Events option, you can disable event logging.

You can use the Event Viewer, located on the Administrative Tools menu, to view events. When the Event Viewer is open, click the DNS log. Any DNS-related events are displayed within the right pane (see Figure 3.14). To view more detailed information about an event, double-click the event within the

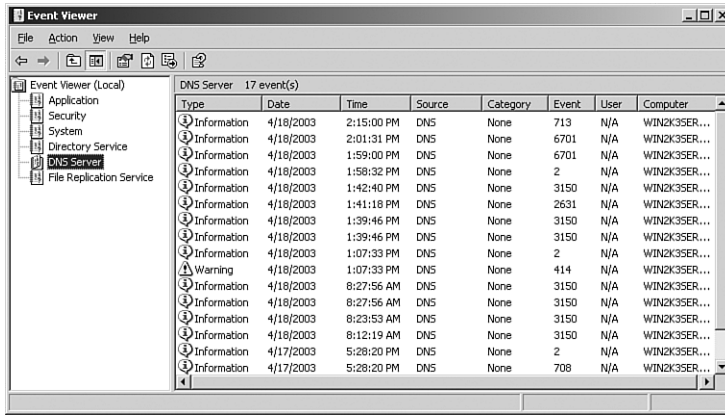


FIGURE 3.14 DNS events are logged in the Event Viewer's DNS log.

right pane. The Properties window for the event displays information such as the date and time the event occurred, the type of event, the user and computer under which the event occurred, and an event ID. A basic description of the event is also provided.

DNS Debug Logging

If you want to collect detailed information about how your DNS server is functioning, you can enable DNS debug logging. Once you do, DNS data will be collected and stored in the `DNS.log` file. Using the Debug Logging tab from the DNS server's properties window, you can choose the type of information that you want logged. For example, you can have all incoming and outgoing packets using TCP logged.

DNS debug logging is not enabled by default. Because it can be resource-intensive and affect server performance, it should only be enabled on a temporary basis.

Replication Monitor

As mentioned earlier in the chapter, zone information can be stored within Active Directory if DNS is installed on a domain controller. This also means that zone updates can be included in Active Directory replication.

Using a tool called Replication Monitor, you can monitor the status of Active Directory replication between domain controllers. If zone information is stored within Active Directory, this also enables you to monitor replication between DNS servers.

Replication Monitor is not installed by default. It can be added by browsing to the `i386\Support\Tools` directory on the Windows Server 2003 CD and running setup. After it is installed, it can be launched from the command prompt using the `Replmon` command.

Troubleshooting DNS

Many of the DNS problems that a network administrator encounters result from missing or incorrect resource records. There are several different tools available that can be used to troubleshoot problems with resource records. These include the following:

- Nslookup
- Dnslint
- Dnscmd

You can run NSLOOKUP with an IP address for a system that you know is outside of your local LAN, or an address that would normally be handled by DNS. NSLOOKUP does the reverse of standard DNS, and should tell you the FQDN that DNS is returning for that particular IP address. If it fails to do so, you need to check DNS connectivity by PINGing the DNS server from a client. You also need to check and make sure that the results of NSLOOKUP are actually valid and true; if they're not, there's a problem with the DNS database and requires some reconfiguration.

NSLOOKUP can be run in two different modes: interactive and noninteractive. If you are looking for a single piece of information, use NSLOOKUP in noninteractive mode. For example, type **`NSLOOKUP 192.168.0.1`** to find the name of the computer. If you need to look up more than one piece of information, use interactive mode.

The Dnslint command-line utility is included in the support tools. It is used to verify the existence and consistency of DNS records. For example, if clients are unable to log on to an Active Directory domain, you can use the command-line utility to verify the existence and the accuracy of the SRV records.

Dnslint will verify the following information and generate a report in HTML format:

- Verifies that all authoritative DNS servers for a domain are responding to queries.

- Verifies that all authoritative DNS servers have synchronized zone data.
- Verifies resource records associated with delegation.

Dnscmd is another command-line utility included in the Windows Server 2003 support tools. It can be used to perform various DNS administrative tasks from the command prompt window. You can use the command to perform the following tasks:

- View and change the properties of a DNS server, zone, or resource record.
- Create and delete zones and resource records.
- Force replication events.

Exam Prep Questions

1. You are the network administrator for your company. All servers are running Microsoft Windows Server 2003. Client computers are running Windows XP Professional.

   Two DNS servers are currently configured on the network that are connected by high-speed WAN connections. Both servers are configured with identical hardware.

   Currently, one server is configured as a primary server and the other is configured as a secondary server. Both DNS servers are upgraded to domain controllers.

   You want to be able to perform updates to the zone data from either DNS server. What should you do?

   - ❍ **A.** In the Properties dialog box for the DNS server, select the General tab and click the Change button beside the zone type. Select the option to store the zone in Active Directory.
   - ❍ **B.** In the Properties dialog box for the zone, select the Zone Type tab and click the Change button. Select the Active Directory–Integrated option.
   - ❍ **C.** In the Properties dialog box for the zone, select the General tab and click the Change button beside the zone type. Select the option to store the zone in Active Directory.
   - ❍ **D.** In the Properties dialog box for the DNS server, select the Zone Type tab and click the Change button. Select the Active Directory–Integrated option.

2. You are the network administrator for your company. All servers are running Microsoft Windows Server 2003. Client computers are running Windows XP Professional.

   You have just finished installing the DNS service on a Windows Server 2003 member server in the bayside.net domain. You need to add a record into the zone file to identify the mail server in the domain.

   What should you do?

   - ❍ **A.** Create a PTR record on the DNS server.
   - ❍ **B.** Create an A record on the DNS server.
   - ❍ **C.** Create a CNAME record on the DNS server.
   - ❍ **D.** Create an MX record on the DNS server.

3. You are the network administrator for your company. Servers have been upgraded to Microsoft Windows Server 2003. Client computers are running Microsoft Windows XP Professional.

The DNS service has been installed on a member server within the company domain. You want to provide fault tolerance for your zone so that name resolution can still continue if the DNS server goes offline. You plan to add another DNS server to the domain. You need to configure the new DNS server role in the appropriate role.

What should you do?

- ❍ **A.** Configure the new server as a secondary DNS server.
- ❍ **B.** Configure the new server as a Master name server.
- ❍ **C.** Configure the new server as a caching-only server.
- ❍ **E.** Configure the new server as a DNS forwarder.

4. You are the network administrator for the Bayside Co. All servers are running Microsoft Windows Server 2003.

Bayside has seven offices located in different parts of the United States. The central office hosts the primary DNS server. All branch office locations have their own DNS servers configured as secondary servers.

The offices are currently connected by slow WAN links, with no plans to upgrade them. The annual budget allows for the addition of a second DNS server at each of the locations. However, you do not want any more traffic generated from zone transfers on the WAN or the local networks.

What should you do?

- ❍ **A.** Configure the new servers as Standard primary DNS servers.
- ❍ **B.** Configure the new servers as Standard secondary DNS servers.
- ❍ **C.** Configure the new servers as Master name servers.
- ❍ **D.** Configure the new servers as Caching-only servers.

5. You are the network administrator for an insurance company. You have upgraded all servers to Microsoft Windows Server 2003. Client computers are running Microsoft Windows XP Professional.

You are trying to determine the hostname associated with the IP address of 192.168.0.20 using the NSLookup command from Wrk02, but you are unsuccessful.

You know the IP address is assigned with Wrk01 and you can successfully resolve other hostnames on the network using this command.

What is most likely the cause of the problem?

- ❍ **A.** There is no A record for Wrk01.
- ❍ **B.** There is no A record for Wrk02.

- ❍ **C.** There is no PTR record for Wrk01.
- ❍ **D.** There is no PTR record for Wrk02.

6. You are the network administrator for the Bayside Company. Domain controllers are running Microsoft Windows Server 2003. Client computers are running Microsoft Windows XP Professional.

A client reports that he is having problems resolving certain hostnames to IP addresses from his computer. You verify that changes have recently been made to some resource records in the zone file. You suspect there are outdated entries in the client resolver cache. The problem is not affecting any other clients on the network

What should you do?

- ❍ **A.** Uninstall the DNS server service.
- ❍ **B.** Delete the `cache.dns` file.
- ❍ **C.** Use the `ipconfig /flushdns` command on the client computer.
- ❍ **D.** Use the Clear Cache option from the Action menu within the DHCP console.

7. You are the network administrator for your organization. You have installed the DNS service on all the Windows Server 2003 domain controllers in the company domain.

Zone information is stored within Active Directory. You want to verify that zone data is being updated between DNS servers.

Which tool can you use to verify this?

- ❍ **A.** System Monitor
- ❍ **B.** Replication Monitor
- ❍ **C.** DNS management console
- ❍ **D.** DNS Debug logging

8. You are the network administrator for a small accounting firm. Domain controllers and member servers are running Microsoft Windows Server 2003. Client computers are running Microsoft Windows XP Professional.

You install the DNS service on two member servers. You need to enable the zone for secure updates. When you open the Property window for the zone, you do not see the Secure Only option.

What could be causing the problem?

- ❍ **A.** You are not logged on as the administrator.
- ❍ **B.** You do not have permission to dynamically update the zone database.

- ❍ **C.** The DNS service is not running on domain controllers.
- ❍ **D.** The zone is configured as a primary zone.

9. You are the network administrator for the Bayside Company. All servers have been upgraded to Microsoft Windows Server 2003.

You have delegated the sales.bayside.net zone to another DNS server on the network. You want to ensure that the name server for bayside.net is notified anytime a new authoritative name server is added to the sales.bayside.net zone.

What should you do?

- ❍ **A.** Using the Name Servers tab from the sales.bayside.net zone, configure the DNS server to notify the DNS server in the parent domain of any changes.
- ❍ **B.** Configure a stub zone on the DNS server within the parent domain.
- ❍ **C.** Configure a DNS server within the bayside.net zone to be a secondary server to the sales.bayside.net zone.
- ❍ **D.** Configure all zones to store information within Active Directory.

10. You are the network administrator for a large insurance company. The primary DNS server is located in the head office.

One of the branch locations has a large number of users. You install a secondary DNS server in this location to decrease name resolution response time.

The WAN link between the branch office and the head office is heavily used.

You want to decrease the number of times that the secondary DNS server checks for zone updates.

What should you do?

- ❍ **A.** In the Properties dialog box for the DNS server, select the Zone Transfers tab and increase the refresh interval.
- ❍ **B.** In the Properties dialog box for the zone, select the Start of Authority (SOA) tab and increase the refresh interval.
- ❍ **C.** In the Properties dialog box for the zone, select the Start of Authority (SOA) tab and increase the retry interval.
- ❍ **D.** In the Properties dialog box for the zone, select the General tab and increase the retry interval.

11. You are the network administrator for your company. All servers have been upgraded to Microsoft Windows Server 2003. Client computers are running Microsoft Windows XP Professional.

You have installed the DNS service on DNSSRV01. You want to configure this DNS server to forward queries that it cannot resolve to another DNS server on the network.

You log on to DNSSRV01 using a user account that belongs to the DNS Admins group. When you display the Forwarders tab in the properties of SRV1 in the DNS console, the option to enable forwarders is unavailable.

What should you do?

- ❍ **A.** Add your user account to the Enterprise Admins group.
- ❍ **B.** Configure DNSSRV01 as a secondary DNS server.
- ❍ **C.** Enable Round Robin on DNSSRV01.
- ❍ **D.** Delete the root DNS zone on DNSSRV01.

12. You are the network administrator for a large company. All network servers are running Microsoft Windows Server 2003. Client computers are running a mixture of Microsoft Windows 95 and Microsoft Windows 2000 Professional.

Your company, contoso.com, has just acquired another company, nwtraders.com. You want to keep the existing network infrastructure. Each domain will maintain its own DNS servers.

You want DNS01, the DNS server for contoso.com, to send DNS queries for hosts in nwtraders.com to DNS01, the DNS server for nwtraders.com domain.

What should you do?

- ❍ **A.** Open the properties window for contoso.com. Use the Forwarders tab to configure DNS01 to forward all name resolution requests to DNS02.
- ❍ **B.** Open the properties window for DNS01. Use the Forwarders tab to configure DNS01 to forward all name resolution requests to DNS02.
- ❍ **C.** Open the properties window for DNS01. Use the Forwarders tab to configure DNS01 to forward all name resolution requests for nwtraders.com to DNS02.
- ❍ **D.** Open the properties window for contoso.com. Use the Forwarders tab to configure DNS01 to forward all name resolution requests for nwtraders.com to DNS02.

13. You are the network administrator for the Bayside Company. You have upgraded all servers to Microsoft Windows Server 2003. Client computers are running Microsoft Windows XP Professional.

All computers are members of a single Active Directory domain called bayside.net. The company website is hosted on three different web servers. The web servers are configured with identical hardware and each one is assigned a unique IP address.

You want traffic to the company website distributed evenly across all three web servers. You open the properties windows for the DNS server.

Which option should you select?

14. You are the network administrator for bcdtrain.com. The network has recently been upgraded to Microsoft Windows Server 2003. Client computers have been upgraded to Microsoft Windows XP Professional.

A new Domain Name System (DNS) server, DNS-01, has been added to the network. This server is configured as the primary DNS server for the bcdtrain.com domain. There is an existing legacy UNIX server on the network, DNS-02, that you configure as a secondary DNS server. You determine that this server is running a version of BIND older than 4.9.4.

You soon discover that DNS-02 is not receiving zone transfers from DNS-01.

What should you do?

- ❍ **A.** Disable the BIND secondaries option on DNS-01.
- ❍ **B.** Enable the BIND secondaries option on DNS-01.
- ❍ **C.** Disable the BIND secondaries option on DNS-02.
- ❍ **D.** Enable the BIND secondaries option on DNS-02.

15. You are a network administrator for your company. The network consists of server computers running Microsoft Windows Server 2003 and client computers running Microsoft Windows XP Professional.

The DNS service is installed on SRV01. It hosts a zone file called contoso.com. SRV02 is configured as an FTP server. The following resource records exist in the zone file for SRV02.

Host (A)

Alias (CNAME)

Service Location (SRV)

Well Known Service (WKS)

You decide to change SRV02 to use Transmission Control Protocol (TCP) port 1021 as the control port for FTP.

You need to ensure that the port is defined correctly in DNS.

Which resource record should you update?

- ❍ **A.** Host (A)
- ❍ **B.** Alias (CNAME)

- ❍ **C.** Service Locator (SRV)
- ❍ **D.** Well Known Service (WKS)

16. You are the network administrator for your company. All servers are running Microsoft Windows Server 2003.

The network consists of several subnets. All clients are WINS-enabled and capable of updating their records dynamically. Each of the subnets has its own WINS server. One of the subnets contains two UNIX servers. Hosts on the local subnet can communicate with the UNIX servers; however, hosts on other subnets are unsuccessful. Clients can resolve NetBIOS names for hosts on other subnets.

Clients on all subnets need to be able to resolve the NetBIOS names of the UNIX servers.

What should you do?

- ❍ **A.** On each of the subnets, configure a secondary WINS server on each subnet.
- ❍ **B.** Configure the WINS servers as replication partners.
- ❍ **C.** Configure the WINS servers to back up their local databases.
- ❍ **D.** Configure static mappings for the two UNIX servers.

17. You are the network administrator for your company. All servers are running Microsoft Windows Server 2003.

The network has a mixture of WINS and non-WINS clients. Three of the seven subnets contain WINS servers. Several users report that they are unable to browse hosts on other subnets. Upon investigating the reports, you discover that the problem is only affecting non-WINS clients.

What should you do?

- ❍ **A.** Configure static mappings for the non-WINS clients.
- ❍ **B.** Install a WINS proxy on each subnet that does not have a local WINS server.
- ❍ **C.** Configure replication between the three WINS servers.
- ❍ **D.** Configure a DHCP relay agent on each subnet.

Answers to Exam Prep Questions

1. C. To change the zone type, right-click the zone within the DNS management console and click Properties. In the Properties dialog box, make sure the General tab is selected and click the Change button beside the zone type. Select the option to store the zone within Active Directory. Answer A is incorrect because the zone type is configured at

the zone level. Answers B and D are incorrect because there is no Zone Type tab available in either the server's Properties dialog box or the zone's Properties dialog box. There is also no option known as Active Directory Integrated.

2. **D.** Mail servers are identified within a zone file using Mail Exchanger (MX) records. Answer A is incorrect because PTR records are used to associate an IP address with its hostname. Answer B is incorrect because A records are used to map hostnames to IP addresses. Answer C is incorrect because CNAME records are used to assign alias names to those names that are already referenced in another record.

3. **A.** The new server should be configured as a secondary server. It will then maintain a copy of the DNS zone file. If the original DNS server goes offline, name resolution can still occur. Answer B is incorrect because master name servers are the source of the zone file for secondary servers. Answer C is incorrect because caching-only servers do not hold any zone information. Answer D is incorrect. A DNS forwarder is not a specific DNS role. When a DNS server is configured as a forwarder, it can forward requests that it cannot resolve to a specific DNS server.

4. **D.** By configuring caching-only servers within each location, you can decrease the name resolution response time for users. Because the caching-only servers do not maintain any zone information, no traffic is generated from zone transfers. Therefore, answers A, B, and C are incorrect.

5. **C.** If the hostname cannot be resolved using the `NSLookup` command, adding a PTR to the zone file will allow you to resolve the IP address to a hostname. Answer B is incorrect because Wrk02 is not the hostname being resolved. Answers A and B are incorrect because A records are used to map hostnames to IP addresses, not vice versa.

6. **C.** By executing the `ipconfig /flushdns` command, you can delete the contents of the client resolver cache on the client computer. Although uninstalling the service would clear the contents of the cache, it's not the easiest way to perform the task; therefore, answer A is incorrect. Answer B is incorrect because deleting the file will completely remove it. Answer D is incorrect because this option is used to clear the contents of the cache file on the DNS server. However, the problem is not affecting any other DNS clients, which indicates that the problem likely resides with the cache on the DNS client.

7. **B.** If the support tools have been installed, you can use Replication Monitor to ensure that replication between DNS servers is occurring on a regular basis. Answer A is incorrect because System Monitor is used to monitor the real-time performance of a DNS server. Answer C is incorrect because the DNS management console is used to configure and manage a DNS server but cannot be used to monitor DNS replication. Answer D is incorrect. DNS debug logging is used to collect detailed information about how a DNS server is operating.

8. **C.** The Secure Only option is available only if the DNS service is installed on a domain controller. Therefore, answers A, B, and D are incorrect. Answer A is incorrect because this would not make the Secure Updates option unavailable. Answer B is incorrect

because dynamic updates are performed when a computer or server updates resource records. Answer D is incorrect because primary and stub zones can be configured for secure updates.

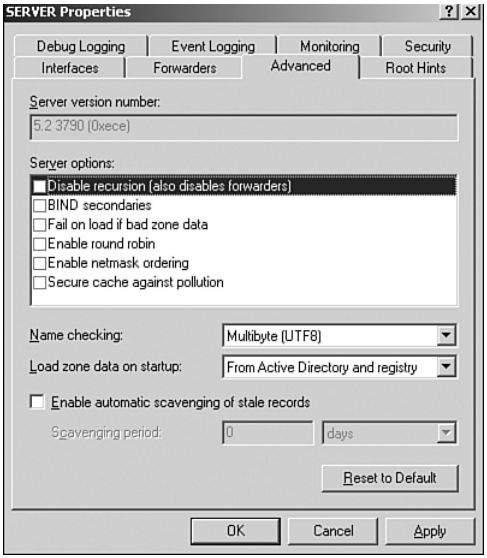
9. **B.** By configuring an authoritative DNS server within bayside.net to host a stub zone for the sales.bayside.net zone, any updates made to the authoritative name server resource records will be updated within the parent zone as well. None of the other options provided remedy this scenario effectively; therefore, answers A, C, and D are incorrect.

10. **B.** To increase the rate at which the secondary server polls for updates, select the Start of Authority (SOA) tab from the zone's Properties dialog box and increase the refresh interval. Answer A is incorrect because the interval at which a secondary server polls for updates is configured at the zone level. Answer C is incorrect because the retry interval defines how often the secondary server continues to poll if the server does not respond. Answer D is incorrect because you must configure the refresh interval, and it must be done from the Start of Authority (SOA) tab.

11. **D.** If a root DNS zone exists on the DNS server, you will not be able to configure a DNS forwarder. You must delete this file before you can proceed. Answer A is incorrect because you do not need to be a member of the Enterprise Admins group to manage a DNS server. Answer B is incorrect because changing the DNS role of the server will not determine whether the DNS server can be a forwarder. Answer C is incorrect because the round robin feature is used to load balance queries across multiple DNS servers.

12. **C.** You should open the properties window for the DNS server called DNS01. Select the Forwarders tab and configure the DNS server to forward any name resolution requests for hostnames in the nwtraders.com domain to DNS02. Answers A and D are incorrect because DNS forwarders are not configured at the zone level. Forwarding must be configured at the server level. Answer B is incorrect because all name resolution requests should not be forwarded to DNS02. Only those requests for hostnames in the nwtraders.com domain should be forwarded to this server.

13. The correct answer is Enable Round Robin. By selecting this option, the DNS server will be able to distribute queries across the web servers. It does so by rotating the list of web servers so a different web server is returned to a client.



14. **B.** You should enable the BIND secondaries option on DNS-01. When this option is enabled, the Windows Server 2003 DNS server will not perform fast zone transfers because it is not supported by versions of BIND older than 4.9.4. Answer A is incorrect. This feature is disabled by default. Answers C and D are incorrect because this feature must be enabled on the Windows Server 2003 DNS server, not on the BIND DNS server.

15. **C.** You should update the SRV record. The SRV record identifies services that are running on a host, the port used by the service, and the protocol. You should not update the Host (A) record. This record identifies the IP address assigned to a host. Answer B is incorrect because an Alias (CNAME) record specifies another DNS domain name for a name that is already referenced in another resource record. Answer D is incorrect because a Well Known Service (WKS) record identifies services running on a host by the service name, not the port number.

16. **D.** To allow hosts on other subnets to resolve the NetBIOS names of the UNIX servers, static mapping must be configured because the UNIX servers are unable to register their NetBIOS records dynamically. Answers A and C are incorrect because performing these tasks does not allow hosts to resolve the NetBIOS names of the UNIX servers. Answer B is incorrect because if the clients can already resolve the names of hosts on other subnets, replication is already configured between the WINS servers.

17. **B.** To allow B-Node broadcasts to be resolved across the network, a WINS proxy agent must be configured. The WINS proxy listens for B-Node broadcasts and contacts the WINS servers on the other subnets to resolve the name resolution request on behalf of the non-WINS client. Therefore, answers A, C, and D are incorrect.

Need to Know More?

Search the online version of TechNet and the Windows Server 2003 Resource Kit using keywords such as "DNS," "Zones," and "Dynamic Updates."

Habraken, Joe. *Sams Teach Yourself Microsoft Windows Server 2003 in 24 Hours.* Sams, 2003. ISBN: 0672324946.

Abbate, Andrew; Kovach, Eric; Morimoto, Rand; Roberts, Ed. *Microsoft Windows Server 2003 Insider Solutions.* Sams, 2003. ISBN: 0672326094.

Williams, Robert; Walla, Mark *The Ultimate Windows Server 2003 System Administrator's Guide.* Addison-Wesley Professional 2003. ISBN: 0201791064.