CHAPTER 5

Configuring DNS Servers

The Domain Name System (DNS) is a distributed database for objects in a computer network. By using a name server approach, the network consists of a hierarchy of autonomous domains and zones. The namespace is organized as a tree that often resembles the organizations that are responsible for the administration boundaries.

The basic function of DNS name servers is to provide data about network objects by answering queries. You can configure the Network Registrar DNS server and zones by accepting the system defaults or changing them through the CLI or GUI.

This chapter assumes that you already installed your software by following the instructions in the *Network Registrar Installation Guide*. It describes the basics of configuring the Network Registrar DNS servers, and their primary and secondary zones. Chapter 6, "Customizing DNS Zone and Server Parameters," describes how to set some of the more advanced zone and server properties.

Table 5-1 lists the topics and sections you need to configure Network Registrar DNS servers.

Table 5-1 DNS Configuration Topics

If you want to...	See...
Know more about DNS before you start configuring your DNS server and zones	Chapter 2, "Understanding Network Registrar Concepts"
Configure the primary name server for a zone	"Configuring a Primary Name Server" section on page 5-1
Configure a secondary zone for the server	"Configuring the Server as a Secondary for a Zone" section on page 5-10
Configure a caching-only server	"Configuring a Caching-Only Server" section on page 5-12
Set the basic DNS server properties	"Setting Basic DNS Server Properties" section on page 5-14
Troubleshoot the DNS server	"Troubleshooting the DNS Server" section on page 5-23

Configuring a Primary Name Server

You do not need to create a loopback zone, because Network Registrar automatically creates one. A loopback zone is a reverse zone that a host uses to resolve its loopback address, 127.0.0.1, to *localhost* so that it can direct network traffic to itself. The reverse loopback zone is 127.in-addr.arpa. If you inadvertently delete the loopback zone, see Appendix D, "Windows 2000 Interoperability."

Adding a Primary Forward Zone

" section on page 5-9 to configure a reverse zone for each network that you use.

Creating the Zone Name

Using the CLI

zone *name* **create primary**

```
nrcmd> zone example.com. create primary server2 hostmaster
```

Importing and Exporting Zone Data" section on page 5-3.

If you need to delete the zone for any reason, use the **zone** *name* **delete** command, and reload the server.

Using the GUI

Step 1 From the Server Manager window (Figure 3-1 on page 3-6), choose the DNS server you want to configure as the primary name server for the zone. If you configure the server on your local host to be the primary name server, choose the *DNS@localhost* object.

Step 2 Click **Add** on the toolbar to display the Add Zone dialog box (Figure 5-1).

Figure 5-1 Add Zone Dialog Box

Step 3 In the Name field, enter the full domain name of the primary zone. End the name with a trailing dot, because it is a fully qualified domain name (FQDN).

Step 4 Choose Primary as the type of zone to add.

Step 5 You may want to import an existing primary zone from a Berkeley Internet Name Domain (BIND) format zone file. See the "Importing and Exporting Zone Data" section on page 5-3. To import a BIND zone file, enter its name in the "Import from BIND file" field, or click **Browse** to locate it.

If you do not want to import the zone file, leave the "Import from BIND file" field blank.

Step 6 Click **OK** to open the Add Primary DNS Zone dialog box, and go on to the "Setting the Zone's Start of Authority" section on page 5-4.

Importing and Exporting Zone Data

The easiest and quickest way to create a primary zone is to import an existing BIND format zone file, defined in RFC 1035. You can also export these same kinds of files to another server.

Importing Using the CLI

To import an existing BIND zone file, create the zone using the **zone** *name* **create primary** command.

```
nrcmd> zone example.com. create primary file=hosts.local
```

Network Registrar can read a BIND named.boot file and import all the zone files identified in it. Use UNIX file path syntax for all operating systems. Also, ensure that any $INCLUDE directives in zone files have absolute file paths. Network Registrar makes any file paths relative to what any *directory* directive contains in the configuration file.

```
nrcmd> import named.boot /etc/named.boot
```

Importing Using the GUI

To import an existing BIND file from the GUI, specify the BIND file name when you add a zone.

Step 1 When entering the primary zone data in the Add Zone dialog box, enter the name of the BIND file or click **Browse** to open a file selection dialog box.

Step 2 Navigate to the zone configuration file location and choose the file. The filename should reflect the zone you are importing. The filename often ends with a .txt or .config file extension.

Step 3 Click **OK**. You should get a series of progress messages in the status bar. Corrupt or unreadable BIND files generate errors. Keep track of any errors so that you can modify the BIND files accordingly.

Step 4 From the Server Manager window (Figure 3-1 on page 3-6), choose the primary zone server that you want to reload. Click **Control** on the toolbar to display the Control dialog box, then **Reload**, then **OK**.

Exporting Zone Data Using the CLI

Exported BIND data can include static or dynamic addresses, or both. When exporting dynamic addresses, Network Registrar includes the MAC address of the host in a text (TXT) resource record for those resource records it creates dynamically. To export a DNS zone, use the **export zone** command to specify the type of addresses (*static*, *dynamic*, or *both*) and the name of the output file. If you specify the filename without a path, the path defaults to the bin directory of the installation directories.

The following example shows partial file output from an **export zone** command. Because host stanley is a DHCP client, its MAC address (from the DHCPREQUEST packet) appears in a TXT record.

```
nrcmd> export zone example.com. static
100 Ok
$ORIGIN example.com.
$TTL 86400
@                       IN      SOA     ns.example.com. hostmaster.example.com. 2 10800
3600 604800 86400
@                       IN      NS      ns.example.com.
moose                   IN      CNAME   moosehorn.example.com.
moosehorn               IN      A       192.168.40.4
ns                      IN      A       192.168.40.3
```

You can also export all zones of a particular type. Use the **export zonenames** command to specify the type (*forward*, *reverse*, or *both*) and output file.

```
nrcmd> export zonenames both hosts.local
```

Exporting UNIX Hosts Files Using the CLI

You can export DNS data in UNIX /etc/hosts file format. Network Registrar combines information from the A and CNAME records for a host. To export all the zones in the server in hosts file format, use the **export hostfile** command and give the name of the output file.

```
nrcmd> export hostfile
100 Ok
# Hostfile created by nrcmd from Network Registrar
# Cisco Systems, Inc.
# Created on Fri Jan 25 15:26:10 Eastern Daylight Time 2002
# 2 records created
#
192.168.40.4    moosehorn.example.com           moosehorn moose         #
192.168.40.3    ns.example.com                  ns                      #
```

Primary Zone Properties in the GUI

The Primary DNS Zone dialog box of the GUI (Figure 5-2) has a number of tabs that relate to the primary zone configuration.

Figure 5-2 Primary Zone Dialog Box Tabs

These tabs are:

- **SOA**—Configures the Start of Authority record for the zone
- **Name Servers**—Configures the authoritative name servers for the zone
- **Hosts**—Configures the hostname-to-address mappings for the zone
- **Zone Transfers**—Allows, disallows, and limits zone transfers from the zone
- **DHCP**—Allows dynamic DNS updates from all or specified addresses
- **Subzones**—Delegates subzones to other servers
- **Resource Records**—Controls the zone's resource records

Setting the Zone's Start of Authority

The Start of Authority (SOA) resource record designates the top of the zone in the DNS inverted-tree namespace. A zone can have only one SOA record, which sets the following primary zone properties:

- Default time to live (TTL)—*defttl*
- Hostmaster (person in charge) name—*person*
- Primary server name—*ns*

- Serial number—*serial*
- Secondary refresh time—*refresh*
- Secondary retry time—*retry*
- Secondary expire time—*expire*
- Minimum TTL—*minttl*

For now, add only the hostmaster and primary server data, the minimum needed to create a zone. For details on other SOA properties, see the "Setting the Zone's SOA Properties" section on page 6-2.

Using the CLI

You used the **zone** *name* **create** command in the "Creating the Zone Name" section on page 5-2. Now use the **zone** *name* **show** or **zone list** command to confirm the zone's SOA properties, or use the **zone** *name* **get** command to get each SOA property separately. You can accept the defaults or explicitly reset them. See the "Setting the Zone's SOA Properties" section on page 6-2. Their default numbered values are:

```
nrcmd> zone example.com. get defttl
nrcmd> zone example.com. get serial
nrcmd> zone example.com. get refresh
nrcmd> zone example.com. get retry
nrcmd> zone example.com. get expire
nrcmd> zone example.com. get minttl
```

Using the GUI

Step 1 When you open the Add Primary DNS Zone dialog box for the first time, the SOA (Start of Authority) tab is active (Figure 5-3). The name of the zone appears in the Name field.

Figure 5-3 SOA Tab (Add Primary Zone Dialog Box)

Step 2 Skip the TTL field for now.

Step 3 In the "Contact email address" field, enter the e-mail address of the zone's hostmaster, the person in charge or administrator of the zone.

Substitute a dot (.) for the "at" symbol (@) that is normally part of the e-mail address, and end the address with a trailing dot (hence, "tom@ns.example.com" becomes "tom.ns.example.com."). Precede any dot before the "at" symbol in the original address with a backslash (\) symbol, so that "tom.marketing@example.com" becomes "tom\.marketing.example.com."

Step 4 In the "Name of primary server" field, enter the name of the primary server. Enter either just the hostname (ns in the example) or the FQDN (ns.example.com. in the example) ending with a trailing dot.

Step 5 Accept the defaults in the remaining fields. These are more advanced settings covered in the "Setting the Zone's SOA Properties" section on page 6-2.

Adding an Authoritative Server for the Zone

Authoritative name servers validate the data in their zones. Both primary and secondary servers can be authoritative. The crucial difference is where they get their zone data. A primary server reads its data from the local database. A secondary server loads its data from the primary server.

Tip You must add at least one name server for a zone. Network Registrar does not consider the zone data complete unless you do so. The name servers you list should be the name servers that you want people outside your domain to query when trying to resolve names in your zone. In the CLI, creating a primary zone requires that you also specify the name server, and it adds it automatically. In the GUI, you must add the name server separately on the Name Servers tab of the DNS Zone dialog box.

You should add the name of the zone's primary server as the authoritative server. This creates a Name Server (NS) resource record for this server in the zone file. You must also add the server's host address. See the "Adding a Host Address for the Primary Server" section on page 5-7.

Using the CLI

When you create the primary zone, this automatically adds the name server. However, you can add further NS records using the **zone** *name* **addRR NS** command. If you remove an NS record, you usually also remove its host record.

Using the GUI

Step 1 On the SOA tab, copy the name of the primary server for the zone in the "Name of primary server" field.

Step 2 Click the **Name Servers** tab (Figure 5-4).

Figure 5-4 Name Servers Tab (Add Primary DNS Zone Dialog Box)

Step 3 Click **Add**.

Step 4 Paste the primary server name into the Name field of the Add Name Server dialog box. If the name is an FQDN, be sure it ends with a trailing dot.

Step 5 Click **OK** to add the name to the Name field of the Add Primary DNS Zone dialog box.

For details on how to add more authoritative servers, see "Configuring the Authoritative Name Servers" section on page 6-6. You must specify a host address for this and any additional name server you add. See the "Adding a Host Address for the Primary Server" section on page 5-7.

If you remove a name server using **Remove**, also remove the host address for it.

Adding a Host Address for the Primary Server

You can add, edit, or remove hosts from a primary zone, and you can establish or change the zone's permanent name-to-IP-address associations. You can also add hosts to reverse zones, and keep the host data up to date as you add and remove hosts. However, you cannot add hosts to secondary zones.

Configuring hosts adds Address (A) resource records for the zone. In this section, you add an A record for each NS record that you added for the zone.

Using the CLI

Use the **zone** *name* **addHost** command to add the authoritative server's hostname and address.

```
nrcmd> zone example.com. addHost ns 192.168.40.2
```

To list the host, use the **zone** *name* **listHosts** command. To remove the host, use the **zone** *name* **removeHost** command. Also, be sure to remove the NS record if the host is a name server. See the "Adding an Authoritative Server for the Zone" section on page 5-6.

Using the GUI

Step 1 In the Add Primary DNS Zone dialog box, click the **Hosts** tab (Figure 5-5).

Figure 5-5 HostsTab (Add Primary DNS Zone Dialog Box)

Step 2 Click **Add**. This opens the Add Host dialog box (Figure 5-6).

Figure 5-6 Add Host Dialog Box (from Hosts Tab)

Step 3 Copy the same primary server name that you copied into the Name Servers tab, into the Name field of the Add Host dialog box, remembering the trailing dot rule.

Step 4 In the Addresses field, enter the IP address of the primary name server. For now, ignore the Aliases and MX records fields and the "Generate reverse mapping records" box.

Step 5 Click **OK** to add the name and address to the Add Primary DNS Zone dialog box.

Confirming Settings and Reloading the Server

Confirm your current primary zone configuration by looking at the resource records that you created.

Using the CLI

Use the **zone** *name* **listRR** command to check the resource records you added. Then, use the **dns reload** command to reload the DNS server with the changes.

```
nrcmd> zone example.com. listRR
100 Ok
Static Resource Records
@     IN     SOA     ns.example.com. hostmaster.example.com
1 10800 3600 604800 86400
@     IN     NS      ns.example.com.
ns    IN     A       192.168.40.2
Dynamic Resource Records

nrcmd> dns reload
```

Using the GUI

Step 1 Click the **Resource Records** tab (Figure 5-7) to verify your zone configuration. Review the resource records created so far. You should see an SOA record for the zone, and an NS and A record for its authoritative name server.

Figure 5-7 Resource Records Tab (Add Primary DNS Zone Dialog Box)

Step 2 Once you are satisfied with the configuration, click **Close**.

Step 3 If you see a red star in the server icon in the Server Manager window, reload the DNS server.

Step 4 If the server traffic signal is missing in the Status Monitor, right-click the server icon and click **Add to status monitor**. The server traffic signal now shows a green light.

Adding a Primary Reverse Zone for the Server

For a correct DNS configuration, you must create a reverse zone for each network that you use. A reverse zone is a primary zone that the DNS server uses to convert IP addresses back to hostnames, and are in a special *in-addr.arpa* domain. You can create a reverse zone manually or import it from BIND.

Using the CLI

Use the **zone** *name* **create primary**, and **zone** *name* **addRR PTR** commands to add the primary reverse zone and pointer record for the server.

```
nrcmd> zone 40.168.192.in-addr.arpa. create primary ns.example.com.
       hostmaster.example.com.
nrcmd> zone 40.168.192.in-addr.arpa. addRR 2 PTR ns.example.com.
```

Import an existing BIND reverse zone the same way you would a forward zone.

```
nrcmd> zone 40.168.192.in-addr.arpa. create primary file=hosts.local
```

Using the GUI

Step 1 Open the Add Zone dialog box (Figure 5-1 on page 5-2) for the same DNS server that you chose for the forward zone. See the "Adding a Primary Forward Zone" section on page 5-2 for the initial steps.

Step 2 Enter the reverse zone name in the Name field. This is the reverse of your zone's network number, added to the special in-addr.arpa domain. Omit any trailing zeroes in the conversion. For example, if your network number is 192.168.40.0, your reverse zone is 40.168.192.in-addr.arpa; if the network number is 192.168.0.0, the reverse zone is 168.192.in-addr.arpa.

Step 3 Choose Primary as the zone type. To import a reverse zone file, see the "Importing and Exporting Zone Data" section on page 5-3.

Step 4 Click **OK** to open the Add Primary DNS Zone dialog box.

Step 5 Enter the same hostmaster and primary server name you entered for the forward zone. Do not enter them as reverse addresses. End any FQDNs with a trailing dot and use the proper hostmaster syntax. Leave the other fields as they are for now.

Step 6 Click the **Name Servers** tab.

Step 7 Enter the same authoritative server as for the forward zone. See the "Adding an Authoritative Server for the Zone" section on page 5-6 for the procedure.

There is no Host tab for a reverse zone. Network Registrar automatically creates all the appropriate host address-to-name entries as you add hosts to the forward zone.

Step 8 Look at your configuration on the Resource Records tab. You should have an NS record and SOA record for the reverse zone. If so, click **Apply**. If not, check that you completed the steps correctly.

Step 9 Reload the DNS server.

Step 10 Look at the Resource Records tab for the reverse zone again. You should see a new pointer (PTR) record for the server host's address. The PTR record name does not end with a dot, because it is relative to the reverse zone's domain name.

Step 11 Click **OK**.

Configuring the Server as a Secondary for a Zone

When you configure a zone, choose at least one secondary server. If you have only one name server and it goes down, there is nothing that can look up names. A secondary server splits the load with the primary or handles the whole load if the primary is unavailable. When a secondary server starts up, it contacts the primary and pulls the zone data over. This is known as a *zone transfer*.

Tip If you have only one secondary server, remove it geographically from the primary. They should not even be on the same network segment, switch, or router, but on a different cluster entirely. See the "General Configuration Guidelines" section on page 1-5.

You can use Network Registrar to configure the DNS server with a secondary zone, which makes the server a secondary for that zone. You also need to give the address of the primary from which to perform zone transfers. Network Registrar must know about this primary server. If you add it to Network Registrar, be sure the secondary zone that you configure is the primary server's primary zone.

Adding a Secondary Forward Zone

Add a secondary zone for a secondary, backup server for a zone.

Using the CLI

Use the **zone** *name* **create secondary** command to create a secondary zone. The IP address you include is that of the primary name server.

```
nrcmd> zone secondary.example.com. create secondary 192.168.41.1
```

To restrict zone transfers to particular addresses only, use the **zone** *name* **enable restrict-xfer** command, then use the **zone** *name* **set restricted-set** command to specify the (comma-separated) addresses.

```
nrcmd> zone secondary.example.com. enable restrict-xfer
nrcmd> zone secondary.example.com. set restricted-set=192.168.1.1,192.168.1.20
```

Using the GUI

Step 1 In the Server Manager window, choose the DNS server to configure as a secondary server for a zone.

Step 2 Click **Add** on the toolbar to display the Add Zone dialog box (Figure 5-1 on page 5-2).

Step 3 Enter the name of the secondary zone in the Name field. This zone can be a subdomain of the domain name that you entered for the primary zone, or it can be in a different domain.

Step 4 Click the **Secondary** box. (You cannot import a secondary zone for a server. However, you can import that same zone as a primary when you configure the primary server.)

Step 5 Click **OK**. This opens the Add Secondary DNS Zone dialog box with the Secondary Zone Configuration tab active (Figure 5-8).

Figure 5-8 Add Secondary DNS Zone Dialog Box

Step 6 Enter the IP address of the primary server from which the zone transfer should occur. This address can be on the same network segment or different network segment.

Step 7 Click the **Zone Transfers** tab (Figure 5-9).

Figure 5-9 Add Secondary DNS Zone (Zone Transfers) Dialog Box

The "Do not restrict zone transfers" box is checked by default. You can restrict zone transfers to specified addresses only by checking the "Restrict zone transfers to the following addresses" box. Then, enter the restricted IP addresses in the fields.

There is no Resource Records tab for a secondary zone, because these records belong to the related primary zone.

Step 8 Click **OK**.

Step 9 Reload the DNS server. Notice that the secondary zone has a different icon than its primary zone.

Adding a Secondary Reverse Zone

You should add a secondary reverse zone, just as you added a secondary forward zone. To add a secondary reverse zone, perform the following steps.

Step 1 Add the secondary reverse zone the same way you did the primary reverse zone, except set the zone type to Secondary. See the "Adding a Primary Reverse Zone for the Server" section on page 5-9.

Step 2 Make the secondary zone's domain name an in-addr.arpa reverse domain, ending it with a trailing dot.

Step 3 Add the same primary server address as for the secondary forward zone and set any zone transfer address restrictions, as in the "Adding a Secondary Forward Zone" section on page 5-11.

Step 4 Reload the DNS server and confirm its status.

Configuring a Caching-Only Server

By definition, all servers are *caching* servers, because they save the data that they receive until it expires. However, you can create a *caching-only* server that is not authoritative for any zone. This type of server's only function is to answer queries by storing in its memory data from authoritative servers. The caching-only server can then learn or cache the data to answer subsequent queries. This can avoid the system overhead required by zone transfers. "Setting Maximum Cache TTL" section on page 6-21 describes setting the cache update frequency.

When you first install Network Registrar to be connected to the Internet, the DNS server automatically becomes a nonauthoritative, caching-only server until you configure zones for it. If you keep the DNS server as a caching-only server, you must have another primary or secondary DNS server somewhere that is authoritative and to which the caching-only server can refer. A caching-only server is never registered on the Internet. In fact, it should never be set up as an authoritative name server for any zone. This can cause *lame delegation*, which occurs when a zone is delegated to a nonauthoritative server. See the "Reporting Lame Delegation" section on page 6-20.

You must set up a caching-only server to respond to *recursive queries*, where a server keeps trying to get to an authoritative server so that it can update its cache with the address resolution data. Because Network Registrar servers are recursive by default, you should just verify that this property is set.

Using the CLI

Use the **dns get no-recurse** command to find out if nonrecursion is disabled. If not, use the **dns disable no-recurse** command.

```
nrcmd> dns get no-recurse
nrcmd> dns disable no-recurse
```

Using the GUI

Step 1 In the Server Manager window, choose the DNS server to designate as caching-only.

Step 2 Click **Show Properties** on the toolbar to display the DNS Server Properties dialog box.

Step 3 Click the **Options** tab (Figure 5-10) and confirm that the "Enable recursive queries" box is checked.

Figure 5-10 Options Tab (DNS Server Properties Dialog Box)

Step 4 Click **OK**.

Step 5 Reload the server to save the changes.

Setting Basic DNS Server Properties

You can set properties for the DNS server itself, along with those you already set for its zones. The Network Registrar GUI provides a Server Properties dialog box (Figure 5-11) for this purpose.

Figure 5-11 General Tab (DNS Server Properties Dialog Box)

The Dialog box is divided into the following tabs:

- **General**—Provides the server name, its cluster name, and the DNS software version. See the "Setting General Server Properties" section on page 5-14.
- **Forwarders**—Sets up forwarders so that the server becomes a forwarding server. See the "Defining Forwarders for the Servers" section on page 5-15.
- **Root Name Servers**—Identifies the root name servers to which the server refers. See the "Defining Root Name Servers" section on page 5-16.
- **Exceptions**—Identifies domains that you want resolved by special servers other than root servers. See the "Specifying an Exception List" section on page 5-17.
- **Options**—Enables and disables options such as recursive and round-robin querying. See the "Setting DNS Server Options" section on page 5-19.
- **Advanced**—Sets the caching interval and other more advanced properties. See the "Setting Advanced Server Properties" section on page 6-19.

Setting General Server Properties

You can display DNS general server properties, such as the name of the server's cluster or host machine and the version number of the Network Registrar DNS server software.

You can change the internal name of the DNS server by deleting the current name and entering a new one. This name is used for notation and does not reflect the server's official name. Network Registrar uses the server's IP address for official name lookups and for dynamic DNS (RFC 2136) updates.

Using the CLI

Use the **dns** [**show**] command to display the DNS server's properties.

```
nrcmd> dns show
```

Using the GUI

Use the General tab in the DNS Server Properties dialog box to display the cluster name and the software version (Figure 5-11 on page 5-14). Change the server name if you wish, then click **Apply**.

Defining Forwarders for the Servers

Sites that must limit their network traffic for security reasons can designate one or more servers to be *forwarders* that handle all off-site requests before the local server goes out to the Internet. Over time, the forwarders build up a rich data cache that can satisfy most requests. They are useful in that they:

- Reduce the load on the Internet connection—Forwarders build up a cache and thus reduce the number of requests sent to external name servers and improve DNS performance.
- Improve the DNS response to repeated queries—The forwarder's cache can answer most queries.
- Handle firewalls—Hosts that do not have access to root name servers can send requests to the forwarder that does.

Tip You may want to restrict the name server even more by stopping it from even attempting to contact an off-site server. A slave server uses forwarders exclusively. It answers queries from its authoritative and cached data, but it relies completely on the forwarders for data not in its cache. If the forwarder does not provide an answer, the slave server does not try to contact other servers.

You can have multiple forwarders. If the first forwarder does not respond after eight seconds, Network Registrar asks each remaining forwarder in sequence until one answers or it gets to the end of the list. If the DNS server does not get an answer, the next step depends on whether you have slave mode on or off:

- If slave mode is on, the DNS server stops searching and responds that it cannot find the answer.
- If slave mode is off, the DNS server sends the query to the domain's designated name servers as if there were no forwarders listed.

Using the CLI

Use the **dns addForwarder** command to specify the address (or space-separated addresses) of name servers you want your Network Registrar DNS server to use as forwarders.

```
nrcmd> dns addForwarder 192.168.40.111
```

Use the **dns enable slave-mode** command to designate the server as a slave.

```
nrcmd> dns enable slave-mode
```

To list the current forwarders, use the **dns listForwarders** command. To edit your forwarder list, you must delete any offending forwarder and re-enter another one. To remove a forwarder or list of forwarders, use the **dns removeForwarder** command.

```
nrcmd> dns listForwarders
nrcmd> dns removeForwarder 192.168.40.111
```

Using the GUI

Step 1 Click the **Forwarders** tab (Figure 5-12) of the DNS Server Properties dialog box.

Figure 5-12 Forwarders Tab (DNS Server Properties Dialog Box)

Step 2 Enter the address or addresses of the forwarder or forwarders. You can replace or delete any entries later on, if necessary.

Step 3 To make the server a slave server, check the "Slave mode" box. Do this if you want the server to rely on its cache and forwarders only.

Step 4 Click **OK**.

Defining Root Name Servers

Root name servers know the addresses of the authoritative name servers for all the top-level domains. When you first start a newly installed Network Registrar DNS server, it uses a set of preconfigured root servers, sometimes called *root hints*, as authorities to ask for the current root name servers.

When Network Registrar gets a response to a root server query, it caches it and refers to the root server list. When the cache expires, the server repeats the process. Because Network Registrar has a persistent cache, it does not need to requery this data when it restarts.

You can also define internal root servers for your network. If you have a large namespace, adding one or more internal root servers is a good solution, even better than using forwarders.

The time to live (TTL) on the official root server records is currently six days, so Network Registrar will requery every six days, unless you specify a lower maximum cache TTL value. See the "Setting Maximum Cache TTL" section on page 6-21 for details.

The root hints list is updated about every six months. You can FTP to ftp.rs.internic.net to get the latest version of the list, or you can run the **nslookup** or **dig** tool. See the "Updating the Root Name Servers List" section on page 5-17 for details.

Adding a Root Name Server

You can add any number of root server names and addresses, but you must configure only valid root name servers. Network Registrar confirms this and displays an error message if any one is invalid.

Using the CLI

Use the **dns addRootHint** command to add root name servers by name and address. Do this only if the server was inadvertently removed from the list or if there was an update to the list since the last version.

```
nrcmd> dns addRootHint a.root-servers.net. 198.41.0.4
```

Using the GUI

The Root Name Servers tab of the DNS Server Properties dialog box contains a set of hints about root name servers.

In the DNS Server Properties dialog box, click the **Root Name Servers** tab (Figure 5-13). Enter the name and address of the root hint server. You can, for example, add an internal root server to the list. (Just be careful not to remove any existing ones.) Then, click **OK**.

Figure 5-13 Root Name Servers Tab (DNS Server Properties Dialog Box)

Updating the Root Name Servers List

Be careful in removing any root servers from the list. If you accidentally remove the address of one of the roots, or you know that it might have changed, use the **nslookup** tool to find out what it is.

```
nslookup a.root-servers.net
Name: a.root-servers.net
Address: 198.41.0.4
```

You can also list the root hint servers using the **dns listRootHints** command. To edit the name or address of a root entry in the DNS Server Properties dialog box, choose it in either column and enter or overtype it. Use the command **dns removeRootHint**, carefully, and add the correct entry using the **dns addRootHint** command.

You can also use the **dig** tool, if it is installed as part of BIND, to update the root servers list.

```
dig @a.root-servers.net . ns
```

Finally, you can FTP to the ftp.rs.internic.net site to get the latest roots list.

```
ftp ftp.rs.internic.net
<login>
ls domain
<roots list>
```

Specifying an Exception List

If you do not want the DNS servers to use the standard resolution method to query the root name server for certain names outside its domain, use *resolution exception*. This bypasses the root name servers and targets a specific server to handle name resolution.

For example, example.com has four subsidiaries: Red, Blue, Yellow, and Green. Each has its own domain under the .com domain. When users at Red want to access resources at Blue, their DNS server knows that it is not authoritative for Blue and appeals to the root name servers. These queries cause unnecessary traffic, and in some cases fail because internal resources are often barred from external queries or sites that use unreachable private networks without unique addresses.

Resolution exception solves these problems. Red's administrator lists all the other example.com domains that users might want to reach and at least one corresponding name server. When a Red user wants to reach a Blue server, the Red server asks the Blue server instead of querying the root.

Adding an Exception

Resolution exception handling is a DNS server property that you can assign.

Using the CLI

Use the **dns listExceptions** command to list the available exceptions. Then, use the **dns addException** command to add the exception domains and servers, separated by a comma.

```
nrcmd> dns listExceptions
nrcmd> dns addException blue.com. 192.168.1.4,192.168.1.7
```

Using the GUI

Step 1 In the DNS Server Properties dialog box, click the **Exception** tab (Figure 5-14).

Figure 5-14 Exception Tab (DNS Server Properties Dialog Box)

Step 2 Click **Add domain name**.

Step 3 Enter the name of the domain you want to add as a resolution exception (Figure 5-15) and click **OK**.

Figure 5-15 Add Domain Name (from Exception Tab)

Step 4 Enter the name server address in the Add Name Server Address dialog box (Figure 5-16) and click **OK**.

Figure 5-16 Add Name Server Address Dialog Box (from Exception Tab)

Step 5 In the DNS Server Properties dialog box, click the **Add address** button to add each additional address, then click **Apply**.

Editing and Removing an Exception

You can edit and remove exception properties from a server.

Using the CLI

To remove a resolution exception, use the **dns removeException** command. To replace it, follow this with a **dns addException** command with the new values. You must also flush the cache so that the server does not refer to the old resolution values in cache. For details, see the "Flushing the DNS Cache" section on page 6-22.

```
nrcmd> dns removeException blue.com.
nrcmd> dns addException blue.com. 192.168.1.8,192.168.1.9
nrcmd> dns flushCache
```

Using the GUI

To remove or change a resolution exception, edit the domain or server address on the Exception tab of the DNS Server Properties dialog box. Choose the address and click the appropriate button, **Edit domain name** or **Edit address**.

To remove a domain name, choose it, then click **Remove domain name**. To remove an address, choose it, then click **Remove address**. If you choose the last remaining address for the domain and try to remove it, clicking **OK** in a confirmation dialog box removes both it and the domain. If you click **Cancel**, you can edit the address or add another one before removing it.

Tip You must complete every resolution exception removal by flushing cache. On the Advanced tab of the DNS Server Properties dialog box (Figure 6-10 on page 6-20), click **Flush now**, then click **OK**. For details, see the "Flushing the DNS Cache" section on page 6-22.

Setting DNS Server Options

You can enable or disable the following DNS server options:

- Recursive and iterative queries
- Round-robin
- Hiding subzones
- Subnet sorting
- Incremental transfer (IXFR)
- NOTIFY

Enabling Recursive Queries

There are two types of queries—*recursive* and *iterative* (nonrecursive). DNS clients typically generate recursive queries, where the name server asks other DNS servers for any nonauthoritative data not in its own cache. With an iterative query, the name server answers the query if it is authoritative for the zone, has the answer in its cache, or tells the client which name server to ask next. You often want to make a root server iterative instead of recursive. Recursion is like saying, "Here is all I know, but I will talk to Bob and get back to you." Iteration is like saying, "Here is all I know, so let me direct you to Bob."

Using the CLI

In the CLI, recursion is set by default. To set iterative queries, enable the *no-recurse* attribute.

```
nrcmd> dns enable no-recurse
```

Using the GUI

In the DNS Server Properties dialog box, click the **Options** tab (Figure 5-10 on page 5-13). Then, if you want to make queries iterative, uncheck the "Enable recursive queries" box.

Enabling Round-Robin

A query might return multiple A records for a name server. To compensate for most DNS clients starting with, and limiting their use to, the first record in the list, you can enable *round-robin* to share the load. This ensures that successive clients resolving the same name will connect to different addresses on a revolving basis. The Network Registrar DNS server then re-arranges the order of the records each time it is queried. It is a method of load sharing, rather than load balancing, which is based on the actual load on the server.

Tip You can adjust the switchover rate from one round-robin server to another using the TTL property of the server's A record. See the "Adding Address, Canonical Name, and Mail Exchanger Records" section on page 6-8.

Using the CLI

Use the **dns get round-robin** command to see if round-robin is enabled (it is by default). If not, use the **dns enable round-robin** command.

```
nrcmd> dns enable round-robin
```

Using the GUI

In the DNS Server Properties dialog box, click the **Options** tab (Figure 5-10 on page 5-13). Check the "Enable round-robin" box to enable round-robin.

Hiding Subzones

For security reasons, you can hide the zone's internal infrastructure from outside the zone. If enabled, it must include the top-level domain. You can enable or disable hiding the subzones using the CLI only.

Using the CLI

Use the **dns enable hide-subzones** command to hide information about the subzone hierarchy for all zones that the server delegates. This collapses a part of the domain namespace into one virtual zone. The default setting is **dns disable hide-subzones**.

```
nrcmd> dns enable hide-subzones
```

Enabling Subnet Sorting

If you enable *subnet sorting*, as implemented in BIND 4.9.7, the Network Registrar DNS server confirms the client's network address before responding to a query. If the client, server, and target of the query are on the same subnet, and the target has multiple A records, the server tries to reorder the A records in the response by putting the target's closest address first in the response packet. DNS servers always return all of a target's addresses, but most clients use the first address and ignore the others.

If you enable both round-robin and subnet sorting, Network Registrar first applies round-robin sorting and then applies subnet sorting. The result is that if you have a local answer, it remains at the top of the list, and if you have multiple local A records, Network Registrar cycles through them.

Using the CLI

Use the **dns enable subnet-sorting** or **dns disable subnet-sorting** (the default) command.

```
nrcmd> dns enable subnet-sorting
```

Using the GUI

On the Options tab of the DNS Server Properties dialog box, check the "Enable subnet sorting" box.

Enabling Incremental Zone Transfers (IXFR)

Incremental zone transfer (IXFR, described in RFC 1995) is a protocol that allows only changed data to be transferred between servers. This is especially useful in dynamic environments. IXFR works together with NOTIFY to ensure more efficient zone updates. See the "Enabling NOTIFY" section on page 5-22.

Using the CLI

Use the **dns enable ixfr-enable** command to enable incremental transfer for all zones for which you did not configure specific behavior. By default, the *ixfr-enable* attribute is enabled.

```
nrcmd> dns enable ixfr-enable
```

Use the following commands to fine tune IXFR:

- **zone** *name* **disable ixfr**—Disables incremental transfer for a single zone if you do not want to use the global value from the **dns disable ixfr-enable** command, unless you override it.

  ```
  nrcmd> zone example.com. disable ixfr
  ```

- **remote-dns** *ipaddr* **create** and **disable ixfr**—Prevents the specified server from performing incremental zone transfers.

  ```
  nrcmd> remote-dns 192.169.1.15 create
  nrcmd> remote-dns 192.169.1.15 disable ixfr
  ```

- **dns set ixfr-expire-interval**—Defines the interval, in seconds, in which to attempt incremental zone transfers, followed by full zone transfers.

  ```
  nrcmd> dns set ixfr-expire-interval=7000
  ```

- **dns enable relax-ixfr-query-validation**—When BIND 8.2.2p5 responds to an IXFR query, it mistakenly responds with the query type AXFR, a full zone transfer. Because Network Registrar adheres to RFC 1995, it expects the value IXFR in that field and rejects the BIND 8.2.2p5 response. You can relax the IXFR query validation by enabling this attribute.

```
nrcmd> dns enable relax-ixfr-query-validation
```

Tip For every optional DNS property you set, you can also unset it using the **dns unset** *attribute* command.

Using the GUI

On the Options tab of the DNS Server Properties dialog box, check the "Enable incremental transfer (IXFR)" box to enable incremental transfer.

Enabling NOTIFY

The NOTIFY protocol, described in RFC 1996, lets the Network Registrar DNS primary server inform its secondaries that zone changes occurred. The NOTIFY packet does not indicate the changes themselves, just that they occurred, and this triggers a zone transfer request. Use NOTIFY in environments where the namespace is relatively dynamic.

Because a zone's master server cannot know specifically which secondary server transfers from it, Network Registrar notifies all registered zone name servers when the zone changes. The only exception is the server named in the SOA primary master field.

Using the CLI

Step 1 To see a list of servers that were set for notification, use the **zone** *name* **get notify-set** command. Use the **dns enable notify** command to send notification for all zones not configured for specific behavior. NOTIFY is enabled by default. You can also enable NOTIFY at the zone level.

```
nrcmd> zone example.com. get notify-set
nrcmd> dns enable notify
```

Step 2 NOTIFY also notifies the servers that you specify in the **notify-set** list. Use the **zone** *name* **set notify-set** command to specify an optional, comma-separated list of servers to notify.

```
nrcmd> zone example.com. set notify-set=1.1.1.1,2.2.2.2
```

Step 3 There are also NOTIFY tuning parameters you can set:

- Time interval to stagger notification of multiple servers of changes; the default is one second.

  ```
  nrcmd> dns set notify-send-stagger=1
  ```

- Minimum interval required before sending notification of consecutive changes on the same zone to a server; the default is two seconds. See the "Fine-Tuning DNS Properties" section on page 5-24 for reasons why you might want to raise the value of this and the *notify-wait* attributes.

  ```
  nrcmd> dns set notify-min-interval=2
  ```

- Time interval to wait, after an initial zone change, before sending change notification to other name servers. The default is five seconds.

  ```
  nrcmd> dns set notify-wait=5
  ```

- Maximum number of changes to accumulate during the notify-wait period. If this number is exceeded, the DNS server sends notification before the notify-wait period passed; the default is 100 changes.

  ```
  nrcmd> dns set notify-defer-cnt=100
  ```

- For secondary zones, the minimum time interval between completing processing one notification and starting another; the default is five seconds.

  ```
  nrcmd> dns set notify-rcv-interval=5
  ```

Using the GUI

On the Options tab of the DNS Server Properties dialog box, check the Enable NOTIFY box.

Troubleshooting the DNS Server

You can troubleshoot the DNS server according to some of the hints and tools described in the following sections.

Useful DNS Troubleshooting Hints and Tools

Useful troubleshooting hints tools to diagnose the DNS server include the following:

- Get the health of the server.

  ```
  nrcmd> dns getHealth
  ```

- List the values of the DNS server properties.

  ```
  nrcmd> dns show
  ```

- Follow any server property changes with a reload.

  ```
  nrcmd> dns reload
  ```

- Choose from the DNS log settings to give you greater control over existing log messages. Use the **dns set log-settings** command in the CLI with one or more of these values (or their numeric equivalents), separated by commas (all are enabled by default except the *scavenge-details* flag):
  - *config* (1)—Server configuration and de-initialization
  - *ddns* (2)—High level dynamic update messages
  - *xfr-in* (3)—Inbound full and incremental zone transfers
  - *xfr-out* (4)—Outbound full and incremental zone transfers
  - *notify* (5)—NOTIFY transactions
  - *query* (6)—Query requests
  - *packet* (7)—General packet processing
  - *datastore* (8)—Datastore processing that provides insight into various events in the server's embedded databases
  - *scavenge* (9)—Scavenging of dynamic resource records
  - *scavenge-details* (10)—More detailed scavenging output (disabled by default)
  - *server-operations* (11)—General high-level server events, such as those pertaining to sockets and interfaces
  - *forward* (12)—Outbound forwarding queries

  - *lame-delegation* (13)—Lame delegation events; although enabled by default, disabling this flag could prevent the log from getting filled with frequent lame delegation encounters.
  - *root-query* (14)—Queries and responses from root servers
  - *ddns-refreshes* (15)—Dynamic DNS update refreshes for Windows 2000 clients
  - *ddns-refreshes-details* (16)—Resource records refreshed during dynamic DNS updates for Windows 2000 clients
  - *ddns-details* (17)—Resource records added or deleted due to dynamic DNS updates.

  Restart the server if you make any changes to the log settings.

- Use the **nslookup** utility to test and confirm the DNS configuration. The utility is a simple resolver that sends queries to Internet name servers. Here are simple commands that return the IP address of the default server and the host. To obtain help for the **nslookup** utility, enter **help** at the prompt after you invoke the command.

```
$ nslookup
> pc3
Server: server2.example.com
Address: 192.168.40.2
Name: pc3.example.com
Address: 192.168.40.33
```

Fine-Tuning DNS Properties

Here are some suggestions to fine-tune some of the DNS server properties:

- **dns set notify-min-interval**—Minimum interval required before sending notification of consecutive changes on the same zone to a server. The default is two seconds. However, you might want to increase this value to exceed the maximum time to send outbound full zone transfers. This accommodates secondary servers that receive inbound incremental zone transfers and send out full transfers to other secondaries. Inbound incremental transfers may abort outbound full transfers. On occasion when secondaries need a full zone transfer, the attribute value should be longer than a typical time to complete an outbound full transfer.
- **dns set notify-send-stagger=5s**—Interval to stagger notification of multiple servers of a change. The default is one second, but you may want to raise it to five.
- **dns set notify-wait=15s**—Time to delay, after an initial zone change, before sending change notification to other name servers. The default is five seconds, but you may want to raise it to 15, for the same reason as given for the *notify-min-interval* attribute.
- **dns set mem-cache-size=1000**—Size of the in-memory record cache, in kilobytes. The default is 200 KB, but you may want to raise it to 1000 KB.
- **dns set neg-cache-ttl=30s**—How long to cache information learned from other name servers about nonexistent names or data. The default is ten minutes, but you may want to lower it to 30 seconds.
- **dns enable lame-deleg-notify**—Network Registrar should notice and log when a DNS server listed in a parent-zone's delegation of subzones does not know that it is authoritative for the zone. This is normally disabled, but you may want to enable it.
- **remote-dns** *address/mask* **create ixfr=true** or **ixfr=false**—Whether you enable or disable incremental transfer, Network Registrar looks for the most specific match, that is, it matches the machine with the longest mask. Use this feature to specify a group of servers with a single command. Note that a netmask of 32 is equivalent to no netmask.