AS/400e

Networking DNS

AS/400e

Networking
DNS

Contents

Part 1. DNS

Domain Name System (DNS) is an advanced system for managing the host names that are associated with Internet Protocol (IP) addresses on TCP/IP networks. Here you will find basic concepts and procedures that you need to know to configure and administer DNS.

Refer to these topics for information about using DNS:

- Install DNS.
- Set DNS authority levels to configure and administer DNS.
- Create DNS data. Create a primary DNS server, secondary DNS servers, convert host tables, and import DNS formatted files to Operations Navigator.
- Access external DNS data: Use forwarders and root servers to access information not in your DNS server's domain.
- Verify DNS function.
- Adminster DNS.
- Troubleshoot DNS problems.

Refer to these topics for information about how DNS works:

- DNS and Simple Mail Transfer Protocol (SMTP).
- DNS domain concepts: This topic provides more information about key DNS concepts, including DNS domains and DNS configuration files.
- Other information about DNS.

Tip: A number of important DNS tasks can be accomplished using AS/400 Operations Navigator. Read how to access AS/400 Operations Navigator. You can access online help for DNS in Operations Navigator after you install an AS/400 connection.

Chapter 1. Print this topic

You can view or download a PDF version of this document for viewing or printing. You must have Adobe® Acrobat® Reader installed to view PDF files. You can download a copy from

http://www.adobe.com/prodindex/acrobat/readstep.html .

To view or download the PDF version, select DNS(about 411 KB or 62 pages).

To save a PDF on your workstation for viewing or printing:

1. Open the PDF in your browser (click the link above).
2. In the menu of your browser, click **File**.
3. Click **Save As...**
4. Navigate to the directory in which you would like to save the PDF.
5. Click **Save**.

Chapter 2. Installing OS/400 DNS

The DNS option (Option 31) does not install automatically with the base operating system. You must specifically select DNS for installation.

To determine whether DNS is installed, follow these steps:

1. At the command line, type **`GO LICPGM`** and press **Enter**.
2. Type **10** (Display installed licensed programs) and press **Enter**.
3. Page down to **5769SS1 OS/400 - Domain Name System**

   If DNS is installed successfully, the **Installed Status** will be ***compatible**, as shown here:

   ```
   LicPgm     Installed Status     Description
   5769SS1    *COMPATIBLE          OS/400 - Domain Name System
   ```
4. Press **F3** to exit the display.

To install DNS, follow these steps:

1. At the command line, type **`GO LICPGM`** and press **Enter**.
2. Type **11** (Install licensed programs) and press **Enter**.
3. Type **1** (Install) in the **Option** field next to OS/400 - Domain Name System and press **Enter**.
4. Press **Enter** again to confirm the installation.

For more information about OS/400 host servers, refer to these topics:

- Starting host servers: The STRHOSTSVR command starts the host server.
- Ending host servers: The ENDHOSTSVR command ends the host server.

Chapter 3. Granting DNS authority

A minimum level of authority is required to allow your AS/400 administrator to configure and administer DNS on AS/400. Completing the procedures below will authorize an administrator to perform the following tasks:

- Create and change existing DNS domain and server configurations.
- Start and stop DNS servers.
- Configure DNS servers to start automatically.

To grant an administrator the proper authorities, refer to these procedures:

- Granting system configuration authority.
- Granting authority to DNS files and directories.
- Granting authority to start the TCP/IP server.

Granting system configuration authority

To grant system configuration authority, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Users and Groups —> All Users**.
2. In the right pane, right-click the administrator's user profile and select **Properties**.
3. Click **Capabilities**.
4. Select **System Configuration**.
5. Click **OK** to close the **Capabilities** dialog.
6. Click **OK** to close the **Properties** dialog.

Granting authority to DNS files and directories

Users will not be able to change DNS configurations they did not create unless they are granted authority to the existing configuration files. When granting authority to an existing DNS configuration, it is necessary to authorize the user profile to the DNS and DNS/TMP directories and configuration files. Getting authority to these files is not a prerequisite to DNS configuration, since the files do not exist until DNS has been configured.

To grant authority to the DNS and DNS/TMP directories, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> File Systems —> Integrated File Systems —> Root —> QIBM —> UserData —> OS400**.
2. Double-click **DNS**.
3. In the right pane, right-click the desired DNS directory and select **Permissions**.
4. Select **Permissions**.
5. Click **Add**.
6. Expand **All Users**.
7. Select the administrator's user profile and click **OK**.
8. Click **Customize**.
9. Click **Select**.

10. Select all of the options that are associated with **Data permissions** and **Object permissions**.
11. Click **OK** to close the **Customize Permissions** dialog.
12. Click **OK** to close the **Permissions** dialog.

To grant authority to existing DNS configuration files, repeat the steps above for BOOT file, CACHE file, and all forward and reverse mapping primary domain (.DB) files.

Note:

> The DNS server will change the ownership of the boot file and the primary domain files (.DB) when the DNS server is started. The QTCP profile will own them. Authorization will *not* be revoked from the *previous owner*. The change of ownership occurs only to prevent the unintentional deletion of the boot file and the primary domain files if the *creator* leaves.

Granting authority to start the TCP/IP server

To grant object authority to the STRTCPSVR and ENDTCPSVR commands, follow these steps:

1. **STRTCPSVR**: At the command line, type `GRTOBJAUT OBJ(QSYS/STRTCPSVR) OBJTYPE(*CMD) USER(ADMINPROFILE) AUT(*USE)`, substituting the name of yo
2. **ENDTCPSVR**: At the command line, type `GRTOBJAUT OBJ(QSYS/ENDTCPSVR) OBJTYPE(*CMD) USER(ADMINPROFILE) AUT(*USE)`, substituting the name of yo

Chapter 4. Creating DNS data

A zone may contain several domains, or it may contain a part of a single domain. Most important, a zone defines an area of DNS responsibility. That responsibility means owning the DNS information about the hosts within the zone. A DNS administrator's main concern is the primary DNS server. A primary DNS server loads a zone's information, such as host names, IP addresses, from disk and has authority over a zone. For information on maintaining DNS data with a primary server, see:

Primary DNS servers
You can create a primary domain by entering the host names manually, or you can import an existing domain file. One way of creating a domain file to import is to convert the local host table.

Secondary DNS servers
Once you have your data in a primary domain on a primary server, you will want to automatically create a copy of that data. You can do this by creating a secondary server on another machine. This will allow you to split the query load between two servers, and provide a backup if the primary server is unavailable.

Converting host tables
This topic outlines the process for converting existing AS/400 host tables into DNS domain files that can be imported using Operations Navigator.

Importing DNS formatted files into Operations Navigator
AS/400 Operations Navigator provides a way to import DNS formatted files. Once they are imported, Operations Navigator can maintain them. It can import existing DNS forward-mapping or reverse-mapping primary DNS domain database files, or files created by the QDNS/QTOBH2N program.

Primary DNS servers

A DNS administrator's main concern is the primary DNS server. A primary DNS server loads a zone's information, such as host names and IP addresses, from disk and has authority over a zone. You can create a primary domain by entering the host names manually, or you can import an existing domain file. You can set up and configure essential primary domains and domain properties through AS/400 Operations Navigator using the procedures below. (If necessary, read how to access AS/400 Operations Navigator.)

Creating primary domains: Select the appropriate method for creating a primary domain based on your configuration requirements.

- To create a primary domain using the DNS Configuration Wizard, follow these procedures:
  1. Configure the primary DNS server
  2. Configure primary domain properties
  3. Add hosts to a domain
- To create a primary domain from an existing domain file, refer to Importing DNS formatted files to Operations Navigator.

- If you have already configured DNS and want to add an additional primary domain, see Configuring additional primary domains.

Modifying DNS properties: These tasks are optional depending on your configuration requirements.

- Add name server records
- Add alias records
- Add host mail exchanger records
- Automatically creating reverse mapping records
- Deleting a primary domain

You may also need to refer to:

- Forward and reverse mapping primary domains: DNS stores host name and IP address information about the hosts in a domain in these two types of files.
- DNS resource records: Resource records record important IP address and host name information.

Configuring the primary DNS server

To configure the primary DNS server using the DNS Name Server Configuration wizard, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, right-click **DNS** and select **Configuration**. If you have not configured DNS before, the **DNS Name Server Configuration** wizard will start automatically.

   Note:

   If you have already configured DNS but want to start over, right-click **DNS** and select **New Configuration**. A warning will display: ″Creating a new configuration will overwrite the existing configuration. Are you sure you want to create a new configuration?″ Click **Yes** to start the **DNS Name Server Configuration** wizard.
3. Click **Next** to bypass the welcome display
4. Click **Next** to bypass the root server display.

   Note: If you are going to add root servers, it is a good idea to add them after completing DNS server configuration.
5. Select **Primary domain server**.
6. Click **Next**.
7. Specify the fully qualified domain name (for example, mycompany.com.) of the primary domain this name server manages.
8. Click **Next**.
9. Click **Add**.
10. In the **Host name** field, enter `localhost`.
11. In the **IP address** field, enter `127.0.0.1 1`
12. Click **OK**.
13. Click **Finish**.

What to do next:

Configure primary domain properties

Configuring primary domain properties

To configure primary domain properties, follow these steps:

1. In the DNS Server Configuration window, expand **DNS Server —> Primary Domains**.
2. Right-click the specific domain you want to configure and select **Properties** to open the **Primary Domain Properties** dialog.
3. Specify the desired data for each page, including: the administrator's e-mail address, create and delete reverse mappings by default (recommended), cache times, additional name servers, domain mail exchangers, and domain data restrictions.
4. Click **OK** to close the **Domain Properties** dialog.

Note: If you select **Create and delete reverse mappings by default**, you will automatically create a reverse-mapping entry every time a new host is added to the primary domain. See Forward and reverse mapping primary domains for more information.

What to do next:

Add hosts to the domain

Adding hosts to a domain

To add a host to a domain, follow these steps:

1. In the DNS Server Configuration window, expand **DNS Server —> Primary Domains** to display the primary domains.
2. Right-click on the specific primary domain (for example, mycompany.com.) in which you want to add a host.
3. Select **New Host** to open the **New Hosts on Primary Domain** dialog.
4. Click **Add**.
5. Enter a fully qualified host name (for example, hostname.mycompany.com.) or a relative host name (for example, host1).
6. Enter an IP address.
7. Enter a mail exchanger name, if desired.

   Note: Using a wild card (example: `*.mycompany.com`) MX records for a domain is not recommended.
8. Enter an alias, if desired.
9. Click **OK** to close the **New Host** dialog.
10. Repeat steps 4–9 for additional new hosts.
11. When finished, click **OK** to close the **New Hosts on Primary Domain** dialog.

    Note: If you selected **Create and delete reverse mappings by default** on the **Primary Domain Properties** page you will automatically create a reverse-mapping entry every time a new host name is added to the primary domain.

Configuring additional primary domains

To configure additional primary domains, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Expand **DNS Server**.
4. Right click **Primary Domains** and select **New Primary Domain**.
5. Enter the fully qualified domain name.
6. Select **Create and delete reverse mappings by default**.
7. Specify any other domain properties using the property pages.
8. Click **OK** to close the **New Primary Domain** dialog.
9. Right-click the your new primary domain and select **Enable**.
10. Close the DNS Server Configuration window.
11. Click **Yes** to save the DNS configuration.

Adding name server records

To add a name server record, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Expand **DNS Server —> Primary Domains** to display the primary domains.
4. Right-click the primary domain you want to change and select **Properties** to open the **Primary Domain Properties** dialog.
5. Select the **Name Servers** tab.
6. Click **Add**.
7. Enter the fully qualified domain name and the host name of the DNS server.
8. Click **OK** to close the **Name Server** dialog.
9. Click **OK** to close the **Primary Domain Properties** dialog.
10. Close the DNS Server Configuration window.
11. Click **Yes** to save the DNS configuration.

Adding alias records

To add an alias record, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Expand **DNS Server —> Primary Domains —> your primary domain** to display the primary domain host entries.
4. Right-click the host entry whose properties you want to change and select **Properties**.
5. Click the **Aliases** tab.
6. Click **Add**.
7. Enter an alias for the host.
8. Click **OK**. This closes the **Host Properties** dialog.
9. Close the DNS Server Configuration window.
10. Click **Yes** to save the DNS configuration.

Adding host mail exchanger records

To add a host mail exchanger record, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Expand **DNS Server —> Primary Domains** to display the primary domains.
4. Click the primary domain to display the host entries for that domain.
5. Right-click the host entry whose properties you want to change and select **Properties**.
6. Click the **Mail** tab.
7. Click **Add**.
8. Enter the host name of the host that will perform mail exchange service for this host.

   Note: Using a wild card (example: `*.mycompany.com`) MX records for a domain is not recommended.
9. Enter a preference value for this mail exchanger record.
10. Click **OK** to close the **Host Mail Exchanger** page.
11. Click **OK** to close the **Host Properties** dialog.
12. Close the DNS Server Configuration window.
13. Click **Yes** to save the DNS configuration.

Automatically creating reverse mapping records

This option causes Operations Navigator to create a reverse mapping primary domain record (PTR resource record) automatically when you add a forward mapping primary domain record. You can activate this option for a primary domain or for a specific host.

To automatically create reverse mapping records for an existing primary domain, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Expand **DNS Server —> Primary Domains** to display the primary domains.
4. In the right pane, right-click the Primary Domain you want to change and select **Properties** to open the **Primary Domain Properties** dialog.
5. On the **General** tab, select **Create and delete reverse mappings by default**.
6. Click **OK** to close the **Primary Domain Properties** dialog.
7. Close the DNS Server Configuration window.
8. Click **Yes** to save the DNS configuration.

To automatically create reverse mapping records for an existing host, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.

3. Expand **DNS Server —> Primary Domains** to display the primary domains.
4. Click the primary domain that contains the host entry you want to change.
5. Right-click the host entry you want to change and select **Properties** to open the **Host Properties** dialog.
6. Click the **Reverse Mapping** tab.
7. Select **Create reverse mapping records for this host**.
8. Click **OK** to close the **Primary Domain Properties** dialog.
9. Close the DNS Server Configuration window.
10. Click **Yes** to save the DNS configuration.

3-byte reverse mapping primary domains

If you enable the **Create and delete reverse mappings by default** box, Operations Navigator automatically creates a 3-byte reverse mapping primary domain if none exists for the host.

Example:

You have a primary domain of mycompany.com and have enabled the **Create and delete reverse mappings by default** check box on mycompany.com's General properties page. You add the host name HOST1, with IP address 1.2.3.4, to the mycompany.com forward mapping primary domain.

Operations Navigator adds this PTR resource record automatically to the reverse mapping primary domain of 4.3.2.in-addr.arpa.:

```
4.3.2.1.in-addr.arpa.  IN    PTR    HOST1.mycompany.com.
```

1-byte and 2-byte reverse mapping domains

Operations Navigator does not create 1-byte or 2-byte network-interface primary domains automatically. If you require a 1-byte (example: 10.in-addr.arpa.) or a 2-byte (example: 110.10.in-addr.arpa.) network interface, you must create new primary domains for them. When you enable the **Create and delete reverse mappings by default** check box, the system adds the PTR (reverse mapping) resource record to the most specific reverse mapping primary domain.

If the new IP address is valid for an existing 3-byte reverse mapping primary domain, a PTR resource record is created in the 3-byte reverse mapping primary domain.

If no valid 3-byte reverse mapping primary domain exists and the IP address of the new host is valid for an existing 2-byte reverse mapping primary domain, a PTR resource record is created in the 2-byte reverse mapping primary domain.

If no valid 2-byte reverse mapping primary domain exists and the IP address of the new host is valid for an existing 1-byte reverse mapping primary domain, a PTR resource record is created in the 1-byte reverse mapping primary domain.

You may also need to refer to:

- Forward and reverse mapping primary domains: DNS stores host name and IP address information about the hosts in a domain in these two types of files.
- Zones of authority: A zone of authority defines an area of DNS responsibility that owns the DNS information about the hosts within the zone.

Deleting a primary domain

To delete a primary domain, follow these steps:

1. In Operations Navigator, expand **your AS/400 server --> Network --> Servers --> TCP/IP**.
2. In the right pane, right-click **DNS** and select **Configuration** to open the DNS Server Configuration window.
3. Expand **DNS Server --> Primary Domains** to display the primary domains.
4. Right-click the primary domain you want to remove and select **Delete**.
5. A warning will display, ″Are you sure you want to delete these 1 items?″ Click **Yes**.

If desired, you can now Import domain data.

Secondary DNS servers

Once you have your data in a primary domain on a primary server, you will want to automatically create a copy of that data. You can do this by creating a secondary server on another machine. This will allow you to split the query load between two servers, and provide a backup if the primary server is unavailable.

A secondary DNS server obtains its domain information from a master DNS server by using a process called a **zone transfer**. Master servers can be primary or secondary DNS servers. Secondary DNS servers query master servers at an interval that is defined on the master DNS server. If the master server's DNS information has been updated, the secondary server starts a zone transfer. This process keeps the zone information of the secondary DNS server synchronized with that of the master server. Securing zone transfers prevents unauthorized DNS servers from loading your zone data.

If you want to add security or alter the default zone transfer times, the information here will describe how to do this on the primary server. Note that these procedures are *optional*. If you choose to alter the transfer times, you will change the system performance as well.

To set up a secondary server, follow these procedures:

- Configure a secondary DNS server: Use this procedure to set up your secondary server using the DNS Name Server Configuration wizard.
- Configure additional secondary domains: Use this procedure to add a secondary domain if you have already configured DNS.
- Securing zone transfers: Use this procedure to prevent any unauthorized DNS server from loading your zone data.

Configuring the secondary DNS server

To configure the secondary DNS server, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, right-click **DNS** and select **Configuration**. If you have not configured DNS before, the **DNS Name Server Configuration** wizard will start automatically.

   Note:

If you have already configured DNS but want to start over, right-click **DNS** and select **New Configuration**. A warning will display: ″Creating a new configuration will overwrite the existing configuration. Are you sure you want to create a new configuration?″ Click **Yes** to start the **DNS Name Server Configuration** wizard.

If you have already configured DNS and want to add a secondary domain, skip to Configuring additional secondary domains.

3. Click **Next** to bypass the welcome display
4. Click **Next** to bypass the root server display.

   Note: If you are going to add root servers, it is a good idea to add them after completing DNS server configuration.
5. Select **Secondary domain server**.
6. Click **Next**.
7. Specify the fully qualified domain name (for example, mycompany.com.) of the primary domain this name server manages.
8. Click **Next**.
9. Enter the IP address of the primary server from which this secondary server will transfer zone data.

   Note: You must use the primary server's IP address; domain names are not accepted.
10. Click **Finish**.
11. Close the DNS Server Configuration window.
12. Click **Yes** to save the DNS configuration.

Configuring additional secondary domains

To configure additional secondary domains, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Expand **DNS Server**.
4. Right click **Secondary Domains** and select **New Secondary Domain**.
5. Specify the fully qualified domain name (for example, mycompany.com.) of the primary domain this name server manages.
6. Click **Add**.
7. Enter the IP address of the primary server from which this secondary server will transfer zone data.

   Note: You must use the primary server's IP address; domain names are not accepted.
8. Select **Save copies of master data**.
9. Click **OK** to close the **New Secondary Domain** dialog.
10. Close the DNS Server Configuration window.
11. Click **Yes** to save the DNS configuration.

Securing zone transfers

This procedure enables only DNS servers that you authorize to load your zone data. This restriction applies to zone transfers only; individual queries remain unrestricted. This controls access to all primary domains that are configured on your system. You can authorize access to specific DNS servers, or to specific networks.

Note: After you create a list of authorized DNS servers, all unauthorized DNS servers are prevented from transferring your zone data.

Restrict access to a specific DNS server

To restrict access to a DNS server, put the DNS server's IP address in the **Secondary server access list** (see procedure below).

Restrict access to a specific network

To restrict access to DNS servers on a specific network, put the network address in the **Secondary server access list**. To restrict access to DNS servers on a subnetwork, put the network address and the subnet mask, in the **Secondary server access list** (see procedure below).

Example of a network address: `12.5.0.0`

Example of a subnet mask: `255.255.255.0`

To create a secure zone transfer access list:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Expand **DNS Server —> Primary Domains** to display the primary domains.
4. Right-click the desired domain and select **Properties**.
5. Select the **Security** tab.
6. Click **Add** to open the **Subnet** dialog.
7. Enter *one* of these options:
   - The **IP address** of an authorized secondary DNS server.
   - The **network address** of an authorized TCP/IP network.
   - The **network address** and the **subnet mask** of an authorized subnetwork.
8. Click **OK** to close the **Subnet** dialog.
9. Click **OK** to close the **Primary Domain Properties** dialog.
10. Close the DNS Server Configuration window.
11. Click **Yes** to save configuration changes.

Converting host tables

A host table includes one record per workstation or network server where each record includes a host name, IP address, and (optional) an alias or more per host. Below is the process for converting existing AS/400 host tables into DNS domain files that can be imported using Operations Navigator. Complete the conversion process at the command line, then import the files in Operations Navigator.

To convert host tables, refer to the following procedures:

1. Use the QDNS/QTOBH2N program to convert existing host table files into DNS formatted files. See:
   - Requirements before running QDNS/QTOBH2N: Before you run QDNS/QTOBH2N, you should complete the steps in this topic.
   - Running QDNS/QTOBH2N to convert host table files: QDNS/QTOBH2N is a program that converts AS/400 host table files into files that are compatible with Operations Navigator DNS Configuration.
   - Example 1: Running QDNS/QTOBH2N: Here is one scenario that gives you an idea of what to expect when you run QDNS/QTOBH2N.
   - Example 2: Running QDNS/QTOBH2N: Here is another scenario that gives you an idea of what to expect when you run QDNS/QTOBH2N.
   - QDNS/QTOBH2N created files: Forward mapping: Running the QDNS/QTOBH2N program creates a single forward mapping primary domain file. You must import this file into Operations Navigator before you can use it.
   - QDNS/QTOBH2N created files: Reverse mapping: Running the QDNS/QTOBH2N program creates a single reverse mapping primary domain file. You must import this file into Operations Navigator before you can use it.
2.

   Go to: Import DNS formatted files in Operations Navigator.

Requirements before running QDNS/QTOBH2N

Carry out this procedure at an AS/400 command line.

QDNS/QTOBH2N

QDNS/QTOBH2N is a program that converts AS/400 host table files into files that are compatible with Operations Navigator DNS Configuration. QDNS/QTOBH2N is in the QDNS library.

Before you run QDNS/QTOBH2N, follow these steps:

1. Grant *ALLOBJ (all object) special authority to the user profile that will run QDNS/QTOBH2N.
2. Add the QDNS library to the current library list with this command:
   ```
   ADDLIBL LIB(QDNS)
   ```
3. Change the coded character set identifier (CCSID) for your job to 37. To change your job CCSID, do this:
   a. Enter `CHGJOB` at the command line but do not press **Enter**.
   b. Press **F4** (Prompt).
   c. Press **F10** (More options).
   d. Page down to the **Coded character set ID** entry.
   e. Write down the existing CCSID value.
   f. Change the CCSID value to **37**.

      Note: Return the CCSID to its original value immediately after you run QDNS/QTOBH2N.
   g. Press **Enter**.

Where to go next:

You are ready to run QDNS/QTOBH2N. See Running QDNS/QTOBH2N to convert host table files for more information.

Running QDNS/QTOBH2N to convert host table files

Carry out this procedure at an AS/400 command line.

Before running QDNS/QTOBH2N see Requirements before running QDNS/QTOBH2N.

QDNS/QTOBH2N program syntax

Here is an example of the syntax used to call the QDNS/QTOBH2N program:

```
call pgm(qdns/qtobh2n) parm('-d' 'DOMAIN' '-n' 'NET' {'options'})
```

Note: All QDNS/QTOBH2N program parameters are case sensitive. You must enter them in lower case. The one exception is the -M optional parameter. You must enter this parameter in upper case.

Required Parameters for QDNS/QTOBH2N

You must specify a value for each of these parameters:

-d DOMAIN
Specify the name of the forward-mapping primary DOMAIN (for example, mycompany.com) that you want to create. Only one -d entry is allowed.

-n NET [:SUBNETMASK]

The -n parameter specifies AS/400 host table entries that will be migrated to DNS formatted files. Substitute a network number (for example: 10.110), for NET, without the trailing zeros. The system allows a maximum of 20 -n options. Each -n entry creates a reverse-mapping primary domain file (h2n.NET). Example:

```
-n 10.110
```

If SUBNETMASK is used, you must provide a network number for the NET value, and a subnetmask number for the SUBNETMASK value. The SUBNETMASK value must be in the format `n.n.n.`, where n is a number from 0 to 255. Example:

```
-n 15.15.16:255.255.248.0
```

Optional parameters for QDNS/QTOBH2N

These parameters are available, but are not required to run QDNS/QTOBH2N:

-c REMOTE-DOMAIN
The -c parameter tells the program to create CNAME records in the default domain for all hosts in DOMAIN. Multiple -c entries are allowed.

-e DOMAIN
The -e parameter tells the program to eliminate all lines from the host table with names in DOMAIN. Multiple -e values are allowed.

-h HOST
The -h parameter tells the program to use HOST in the fields of the start of authority (SOA) record that require hostnames. The default is the host on which you run the QDNS/QTOBH2N program.

-m WEIGHT:MX-HOST

The -m parameter tells the program to include a mail exchanger (MX) record for each host in your domain pointing to MX-HOST at WEIGHT. Multiple -m WEIGHT values are allowed.

-s SERVER

The -s parameter tells the program to list SERVER in each domain's NS records. Multiple -s values are allowed.

-t The -t parameter tells the program to create text (TXT) records from the text description section of an AS/400 host table entry.

-M The -M parameter tells the program to create no MX records. By default, the program QDNS/QTOBH2N creates an MX record for each host name in DOMAIN. You must enter this option in upper case.

QDNS/QTOBH2N Operation Notes

When running QDNS/QTOBH2N, you should consider these points:

- By default, QDNS/QTOBH2N creates an MX record with a preference (or weight) value of 10 for each host in the file. The MX record points to the host itself as the mail exchanger.
- You can stop the creation of MX records with the -M option.
- A maximum of 5000 AS/400 host table entries can be converted by the QDNS/QTOBH2N program for each job.
- Existing entries in the files, h2n.DOMAIN and h2n.NET, are overwritten each time the QDNS/QTOBH2N program runs. The data in the new file entries is specified by the parameters of the QDNS/QTOBH2N program.
- This message displays when the QDNS/QTOBH2N program completes successfully:

  ```
  Process completed successfully.  DNS formatted
  file prefixed by h2n built in directory
  /QIBM/UserData/OS400/DNS.
  ```

Where to go next:

- Example 1: Running QDNS/QTOBH2N: Here is a scenario that gives you an idea of what to expect when you run QDNS/QTOBH2N.

Example 1: Running QDNS/QTOBH2N

This scenario gives you an idea of what to expect when you run QDNS/QTOBH2N.

Suppose that an AS/400 host table contained these entries:

```
       10.110.42.1     host1
       10.110.42.2     host2.mycompany.com
                           host2alias.mycompany.com
       10.110.42.3     host3.mycompany.com.
       10.110.69.1     host4.mycompany.com
       10.110.69.2     host5.othercompany.com.
       10.5.24.1       host6.mycompany.com.
       10.5.24.2       host7.mycompany.com
```

Suppose that the name of the new DOMAIN to be created is mycompany.com. Suppose that the network interface addresses (NET) to be migrated from an AS/400 host table are 10.110.42 and 10.110.69.

The QDNS/QTOBH2N program call would look like this:

```
   call pgm(qdns/qtobh2n) parm('-d' 'mycompany.com' '-n'
   '10.110.42' '-n' '10.110.69')
```

If the program runs successfully, these three files are created in the Integrated File System directory /QIBM/UserData/OS400/DNS:

```
   h2n.mycompany
   h2n.10.110.42
   h2n.10.110.69
```

The contents of each file are as follows:

File contents: h2n.mycompany

```
mycompany.com.IN SOA as400hostname.mycompany.com.
    postmaster.as400hostname.mycompany.com.(
    1 10800 3600 604800 86400)


mycompany.com.          IN  NS     as400hostname.mycompany.com.
localhost               IN  A      127.0.0.1
host1                   IN  A      10.110.42.1
host1                   IN  MX       10 host1.mycompany.com.
host2                   IN  A      10.110.42.2
host2alias              IN  CNAME   host2.mycompany.com.
host2                   IN  MX      10 host2.mycompany.com.
host3                   IN  M      10.110.42.3
host3                   IN  MX      10 host3.mycompany.com.
host4                   IN  A      10.110.69.1
host4                   IN  MX       10 host4.mycompany.com.
host5.othercompany.com  IN  A      10.110.69.2
host5.othercompany.com  IN  MX   10.host5.othercompany.com.mycompany.com.
```

File contents: h2n.10.110.42

```
42.110.10.IN-ADDR.ARPA. IN  SOA  as400hostname.mycompany.com.
    postmaster.as400hostname.mycompany.com.(
    2 10800 3600 604800 86400 )

              IN  NS     as400hostname.mycompany.com.
1.42.110.10.IN-ADDR.ARPA.   IN  PTR   host1.mycompany.com.
2.42.110.10..IN-ADDR.ARPA.  IN  PTR   host2.mycompany.com.
3.42.110.10.IN-ADDR.ARPA.   IN  PTR   host3.mycompany.com.
```

File contents: h2n.10.110.69

```
69.110.10.IN-ADDR.ARPA. IN  SOA as400hostname.mycompany.com.
    postmaster.as400hostname.mycompany.com. (
    2 10800 3600 604800 86400 )

              IN  NS    as400hostname.mycompany.com.
1.69.110.10.IN-ADDR.ARPA. IN PTR  host4.mycompany.com.
2.69.110.10.IN-ADDR.ARPA. IN PTR  host5.othercompany.mycompany.com.
```

Example 1 Notes:

Information for AS/400 host table entries host6 and host7 are not included in the files created by the QDNS/QTOBH2N program. The IP addresses associated with these host names, 10.5.24.1 and 10.5.24.2, are not part of the network numbers that are specified with the -n option, 10.110.42, and 10.110.69.

The host name **localhost** with IP address **127.0.0.1** is included in h2n.mycompany. This special address is included as an entry in every h2n.DOMAIN file that is created. This is also known as the **loopback** address.

The AS/400 host table entry with the fully qualified name host5.othercompany.com.mycompany.com. is included in h2n.mycompany as host name host5.othercompany.com.mycompany.com.

Where to go next:

- Example 2: Running QDNS/QTOBH2N: Here is another scenario that gives you an idea of what to expect when you run QDNS/QTOBH2N.

Example 2: Running QDNS/QTOBH2N

This scenario gives you an idea of what to expect when you run QDNS/QTOBH2N.

Suppose that an AS/400 host table contained these entries:

```
10.110.42.1     host1
      Text 'description':   Text Text Text Text and more Text.
10.110.42.2     host2
                host2alias1
10.110.42.3     host2
                host2alias2
10.5.24.1         host3
```

For this example, let us suppose the following:

- The name of the new DOMAIN to be created is **mycompany.com.**
- The only network interface address (NET) to be migrated from an AS/400 host table is **10.110.42.**
- No mail exchanger (MX) records are to be created.
- The text description section of AS/400 host table entries is to be converted to TXT records.

The QDNS/QTOBH2N program call would look like this:

```
call pgm(qdns/qtobh2n) parm
('-d' 'mycompany.com' '-n' '10.110.42' '-t' '-M')
```

If the program runs successfully, these two files are created in the Integrated File System directory /QIBM/UserData/OS400/DNS:

```
h2n.mycompany
h2n.10.110.42
```

The contents of each file are as follows:

File contents: h2n.mycompany

```
mycompany.com. IN SOA as400hostname.mycompany.com.
    postmaster.as400hostname.mycompany.com.(
    1 10800 3600 604800 86400)

host1            IN    A       10.110.42.1
host1            IN    TXT   "Text Text Text and more Text."
host2            IN    A       10.110.42.2
host2alias1      IN    A       10.110.42.2
host2            IN    A       10.110.42.3
host2alias2      IN    A       10.110.42.3
```

File contents: h2n.10.110.42

```
42.110.10.IN-ADDR.ARPA. IN  SOA  as400hostname.mycompany.com.
    postmaster.as400hostname.mycompany.com. (
    2 10800 3600 604800 86400 )
```

```
1.42.110.10.IN-ADDR.ARPA.      IN  PTR   host1.mycompany.com.
2.42.110.10.IN-ADDR.ARPA.      IN  PTR   host2.mycompany.com.
3.42.110.109.IN-ADDR.ARPA.     IN  PTR   host2.mycompany.com.
```

Example 2 Notes:

- No mail exchanger (MX) records are included in h2n.mycompany. The -M option tells the program not to create MX resource records.
- A text (TXT) resource record is included in h2n.mycompany. The -t option tells the program to convert the information in the text description section of an AS/400 host table entry to a TXT resource record.
- Two address (A) records are included for AS/400 host table entry host2 in h2n.mycompany. This is because host2 has two AS/400 host table entries, each with a different IP address.
- Two address (A) records are included for host2 in h2n.mycompany. Both AS/400 host table entries are associated with the same IP address. When migrated, both host2 records and their associated aliases will result in the creation of address (A) records. No CNAME records are created.

Accessing DNS functions through AS/400 Operations Navigator: **Tip**: A number of DNS procedures are available in the online help from AS/400 Operations Navigator. You can access TCP/IP online help for DNS in Operations Navigator after you install an AS/400 connection.

To access the graphical user interface for DNS in Operations Navigator, follow this path:

1. Open the Client Access folder on your desktop.
2. Open Operations Navigator.
3. Expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
4. In the right pane, right-click **DNS** and select **Configuration** to open the DNS Server Configuration window.

   Note:

   - If you have not already configured DNS, the **DNS Name Server Configuration** wizard will automatically start.
   - If you have already set up the DNS Name Server, you can right-click a server or domain and select **Properties** to edit the properties pages.

For additional information, you can view the online help by clicking the **Help**. You can also drag-and-drop the question mark onto a field for help.

Importing DNS formatted files to Operations Navigator

AS/400 Operations Navigator provides a way to import DNS formatted files. Once imported, Operations Navigator can maintain these files. It can import existing DNS forward-mapping or reverse-mapping primary DNS domain database files, or files created by the QDNS/QTOBH2N program.

Import domain data will create the primary domain for you. If a primary domain with that name has already been created, you must delete that primary domain before importing domain data. If you have never configured DNS before, you must first create a cache-only server to access the DNS Server Configuration window.

To import a DNS-formatted file to Operations Navigator, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, right-click **DNS** and select **Configuration**.

3. Expand **DNS Servers**.
4. Right-click **Primary Domains** and select **Import domain data** to open the **Import domain data** dialog.
5. Enter the integrated file system path, followed by the name of the file that you want to import. The default path (/QIBM/UserData/OS400/DNS) is already displayed.

   Example: If the name of the primary forward mapping domain database file you want to import is h2n.mycompany, and it is located in the Integrated File System directory **/QIBM/UserData/OS400/DNS**, enter:

   ```
   /QIBM/UserData/OS400/DNS/h2n.mycompany
   ```
6. Click **OK** to close the **Import domain data** dialog.
7. Close the DNS Server Configuration window.
8. Click **Yes** to save the DNS Configuration.

Primary domain file names

The Import domain data function creates a new primary domain on the DNS Server Configuration window under Primary Domains. The name displayed under Primary domain is determined in one of two ways:

- If the Start of Authority (SOA) resource record contains a fully qualified domain name, this fully qualified domain name is used as the name of the primary domain. If necessary, you can edit the SOA record and add the fully qualified domain name before running the import domain data function.
- If the SOA record does not contain a fully qualified domain name, the name of the file being imported (example: `h2n.mycompany`) is used as the name of the primary domain.

Record validation

The Import domain data function reads and validates each record of the file that is being imported.

Import domain data continues processing the next record in the file. After the Import domain data function has finished, the records associated with the lines in error can be examined individually.

Note:

- Importing a very large primary domain may take several minutes.
- The Import domain data function does not support the $include directive. Import domain data’s validity checking process identifies lines that contain the $include directive as lines in error.

QDNS/QTOBH2N created files: Forward mapping

The QDNS/QTOBH2N program creates two types of files:

- Forward mapping primary domain data files
- Reverse mapping primary domain data files

Forward mapping primary domain data files

Running the QDNS/QTOBH2N program creates a single forward mapping primary domain file. The forward mapping primary domain file is created in the Integrated File System directory:

```
/QIBM/UserData/OS400/DNS
```

The name of the file is:

```
h2n.first-label-in-DOMAIN.
```

where **first-label-in-DOMAIN** is the first label of the DOMAIN name specified after the -d parameter.

For example, if the DOMAIN name was **mycompany.com**, the first-label-in-DOMAIN is:

```
mycompany.
```

The forward mapping primary domain file created by the QDNS/QTOBH2N program is:

```
h2n.mycompany.
```

Note: You must import this file into AS/400 Operations Navigator before you can use it. Use the Operations Navigator Import domain data function to import the file. In the above example, the file you import would be:

```
/QIBM/UserData/OS400/DNS/h2n.mycompany.
```

QDNS/QTOBH2N created files: Reverse mapping

The QDNS/QTOBH2N program creates two types of files:

- Reverse mapping primary domain data files
- Forward mapping primary domain data files

Running the QDNS/QTOBH2N program creates a single reverse mapping primary domain file. The file is created in the Integrated File System directory:

```
/QIBM/UserData/OS400/DNS
```

The name of the file is:

```
h2n.NET.
```

where the **NET** value is the network number specified after each -n parameter. A separate file is created for each network number that is specified after an -n parameter.

For example, if the network number is **10.110.42**, the QDNS/QTOBH2N program creates a reverse mapping primary domain file named:

```
h2n.10.110.42.
```

Note: You must import this file into AS/400 Operations Navigator before you can use it. Use the Operations Navigator Import domain data function to import the file. In the above example, the file you import would be:

```
/QIBM/UserData/OS400/DNS/h2n.10.110.42
```

Chapter 5. Accessing external DNS data

How do you gain access to information that does not reside on your local systems? DNS servers can manage tasks such as: obtaining domain information from authoritative servers, and storing answers to queries received. For what you need to know about accessing external DNS data, see:

- DNS forwarders: A forwarder is commonly used when AS/400 DNS server is located on the secure side of a Firewall.
- DNS root servers: Root servers are used by a DNS server that is directly connected to the Internet.
- Cache-only DNS servers: A cache-only DNS server obtains all DNS information from other DNS servers.

DNS forwarders

A forwarder is commonly used when AS/400 DNS server is located on the secure side of a Firewall. An AS/400 DNS server is configured to be authoritative over the secure part of the network (or intranet). The Firewall provides the only access to the Internet. When a DNS server on the secure side of the Firewall receives a query for information outside of its zone of authority, it sends the query to the DNS server on the Firewall. The DNS server running on the Firewall resolves the query and returns the answer back to the DNS server on the secure side of the Firewall. In this arrangement the DNS server on the secure side of the Firewall is configured to use a forwarder; the DNS server on the Firewall is configured to use root servers.

To create a forwarder, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Right-click **DNS Server** and select **Properties** to display the **DNS Server Properties** dialog.
4. Click the **Forwarders** tab.
5. Click **Add**.
6. Enter the IP address of the forwarder.

   Note: You may add additional forwarders by repeating the previous two steps.
7. Click **OK** to close the **DNS Server Properties** dialog.
8. Close the DNS Server Configuration window.
9. Click **Yes** to save the DNS configuration.

DNS root servers

Root servers are critical to the function of a DNS server that is directly connected to the Internet. DNS servers must use root servers in order to answer queries about hosts other than those that are contained in their own domain files. Its domain files contain information only about hosts within the DNS server’s domain.

To reach out for more information, a DNS server has to know where to look. On the Internet, the first place a DNS server looks is the root servers. The root servers direct a DNS server towards other servers in the hierarchy until an answer is found, or it is determined that there is no answer.

Operations Navigator's 'Load defaults' list

Operations Navigator supplies a list of Internet root servers. You should use Internet root servers only if your DNS server is connected directly to the Internet. The default list is current when Operations Navigator is released. You can use the default list to get a DNS server running. You should compare the root server addresses in the default list to the list on the InterNIC site as soon as possible. Update your configuration's root server list from the InterNIC site if the list has changed. See the AS/400 Operations Navigator **Adding root servers** procedure for instructions on loading the default list. (Read how to access AS/400 Operations Navigator.)

Where to get Internet root server addresses

The top-level root server's addresses change from time to time, and it is the DNS administrator's responsibility to keep them current. InterNIC maintains a current list of Internet root server addresses. To obtain a current list of Internet root servers, follow these steps:

1. Anonymous FTP to the InterNIC server: `FTP.RS.INTERNIC.NET`
2. Download this file: `/domain/named.root`
3. Use the AS/400 Operations Navigator **Adding root servers** procedure to add the updated list of Internet root servers to your primary domain configuration. (Read how to access AS/400 Operations Navigator.)

A DNS server behind a firewall may have no root servers defined. In this case, the DNS server can resolve queries only from entries that exist in its own primary domain database files, or its cache. It may forward off-site queries to the firewall DNS. In this case, the firewall DNS server acts as a forwarder.

Cache-only DNS servers

All DNS servers cache answers to queries they receive from outside their own zone of authority. A cache-only DNS server obtains all DNS information from other DNS servers. It does not use host information in domain files and does not perform zone transfers. A cache-only DNS server must have at least one root server or forwarder listed, or it cannot resolve domain names. It stores the answer to each query in its cache for later use. A cache-only DNS server is not authoritative for any zone.

If DNS has never been configured, setting up a cache-only server is necessary in order to import domain data.

To create a cache-only server, follow these steps:

1. In Operations Navigator, expand **your AS/400 server** —> **Network** —> **Servers** —> **TCP/IP**.
2. In the right pane, right-click **DNS** and select **Configuration**. If you have not configured DNS before, the **DNS Name Server Configuration** wizard will start automatically.

   Note:

If you have already configured DNS but want to start over, right-click **DNS** and select **New Configuration**. A warning panel will display: ″Creating a new configuration will overwrite the existing configuration. Are you sure you want to create a new configuration?″ Click **Yes** to start the **DNS Name Server Configuration** wizard.

3. Click **Next** to bypass the welcome display
4. Click **Next** to bypass the root server display.
5. Select **Cache-only server**.
6. Click **Finish**.

Chapter 6. Verifying DNS server function

To verify that your DNS server is functioning properly, follow these steps:

1. Enable primary domains.
2. Start the DNS server.
3. Check the job log for DNS server messages.
4. Verify DNS function with NSLookup.
5. Configure DNS for TCP/IP.

Enabling and disabling domains

To enable a domain, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Expand **DNS Server —> Primary Domains** to display the primary domains.
4. Right-click the specific domain you want to enable or disable and select **Enable**.
5. Close the DNS Server Configuration window.
6. Click **Yes** to save the DNS configuration.

To disable a domain, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Expand **DNS Server —> Primary Domains** to display the primary domains.
4. Right-click the specific domain you want to enable or disable and select **Disable**.
5. Close the DNS Server Configuration window.
6. Click **Yes** to save the DNS configuration.

Starting and stopping the DNS server

To start your DNS server, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, the current status will be displayed in the **Status** column next to DNS.

   Right-click **DNS** and select **Start**.

To stop your DNS server, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, the current status will be displayed in the **Status** column next to DNS.

Right-click **DNS** and select **Stop**.

Checking the job log

Check the job log to verify that the DNS server started, loaded its information, and is ready to answer queries. Any error messages will also be displayed in the job log.

To check the job log for DNS server messages, follow these steps:

1. At the command line, type `WRKACTJOB JOB(QTOBDNS)` and press **Enter**.

   The job looks like this:

   ```
   Subsystem/Job  User    Type  CPU%   Function     Status
   QTOBDNS        QTCP    BCH    00    PGM-QTOBDNS   SELW
   ```
2. Type **5** (Work with) in the **Opt**ion field and press **Enter**.
3. Type **10** (Display job log) and press **Enter**.
4. Press **F10** (Display detailed messages).

This displays the information and error messages in the job log.

Standard messages include:

```
call pgm(qdns/qtobdns) parm('-p' '53' '-d' '0'
'-b''/QIBM/UserData/OS400/DNS/BOOT')
DNS server starting.
primary zone mycompany.com. (serial number 8723452)
loaded successfully.
primary zone 0.0.127.in-addr.arpa (serial number 8723453)
loaded successfully.
cache zone. (serial number 0 ) loaded successfully.
Ready to answer queries.
```

The preceding messages show that the DNS server has started and is ready to answer queries.

Job log error messages

The job log also contains error messages, if any, concerning the DNS server. Here are some of the error messages you might encounter:

```
Primary domain mycompany.com disabled.
```

This indicates that the primary domain needs to be enabled.

```
Could not open boot configuration file
/QIBM/UserData/OS400/DNS/BOOT.
```

This may indicate that no DNS configuration files have been created, or that the DNS option has not been installed on the system.

Verifying DNS function with NSLookup

Use NSLookup (Name Server Lookup) to query the DNS server for an IP address. This verifies that the DNS server is responding to queries. Request the host name that is associated with the loopback IP address (127.0.0.1). It should respond with the host name (localhost).

To verify DNS function with NSLookup, follow these steps:

Note: Have you not yet configured your AS/400 to use your new server? Is the configured server not available? Do you want to direct NSLOOKUP to another server? Then press **F4** to enter an address for the parameter Domain Name Server(NSLOOKUP DMNNAMSVR(0.0.0.0)).

1. At the command line, type `NSLOOKUP` and press **Enter**.

   This starts an NSLookup query session.
2. Type **server** followed by your server name and press **Enter**. For example:

   ```
   server as400name.mycompany.com
   ```

   Substitute your domain name for *as400name.mycompany.com*

   This information displays:

   ```
     Server:  as400name.mycompany.com
     Address: n.n.n.n
   ```

   Your DNS server’s IP address is substituted for *n.n.n.n*
3. Enter `127.0.0.1` on the command line and press **Enter**.

   This information should display, including the loopback host name:

   ```
      > 127.0.0.1
     Server:  as400name.mycompany.com
     Address:  n.n.n.n

     Name:    localhost
     Address:  127.0.0.1
   ```

The DNS server is responding correctly if it returns the loopback host name: **localhost**.

If you need help, type `?` and press **Enter**.

Type `exit` and press **Enter** to quit the NSLOOKUP terminal session.

Configuring DNS for TCP/IP

To configure DNS on TCP/IP so that it can be used by TCP/IP applications on the AS/400, follow these steps:

1. In Operations Navigator, expand **your AS/400 server --> Network --> Protocols**.
2. In the right pane, right-click TCP/IP and select **Properties**.
3. Click the **Host Domain Information** tab.
4. Click **Add** and enter up to three DNS IP addresses.
5. In the Search Order field, select **Search host table first** or **Search name server first**. If you are not sure which to choose, refer to Local host table versus Domain name server.
6. Click **OK** to close the **TCP/IP properties** dialog.

Chapter 7. Administering DNS servers

Once you have created your servers, you need to activate them and verify that they are working. You can then configure your AS/400 to use your servers. You can track and verify that your DNS server on AS/400 is functioning properly by using a variety of logs, statistics, and debug features. DNS server statistics can help you determine the work load and performance. The DNS server database can provide useful information to diagnose problems. For what you need to know about administering DNS servers, see:

- Activating the DNS server log
- Viewing the DNS server log
- Viewing DNS server statistics
- Viewing the DNS server database dump: The DNS server database can provide useful information that might help diagnose a DNS server problem, or to determine that the DNS server is performing correctly.
- Backing up DNS configuration files and maintaining log files: Here are details on the configuration and database files that you should be backing up.
- Local host table versus Domain name server: Address resolution by way of a domain name system server is not necessarily preferable over resolution by way of the local host table. The local host table and the DNS can be used together. IBM recommends careful use of both. Here is an overview of the important considerations.

Activating the DNS server log

Once the DNS server log is activated, all queries received by the DNS server will be written to the QUERYLOG file in the DNS directory.

To activate the DNS server log, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Right-click **DNS Server** and select **Properties**
4. Select the **Options** tab.
5. Click the **Log all queries received by name server** box.
6. Click **OK** to close the DNS Server Properties dialog
7. Right-click **DNS Server** and select **Update Server**.
8. Close the DNS Server Configuration window.
9. Click **Yes** to save configuration changes.

Note: The QUERYLOG file continues to grow in size as long as the DNS server continues to run. It is a good idea to delete the file from time to time to keep it from taking up too much disk space. See Viewing the DNS server log for information about accessing the file.

Viewing the DNS server log

After the DNS server log has been activated, all queries received by the DNS server will be written to the log.

To view the DNS server log, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> File Systems —> Integrated File Systems —> Root —> QIBM —> UserData —> OS400 —> DNS —> QUERYLOG**.
2. Select **Notepad** from the list of applications.
3. Click **OK**.

This opens the DNS server log in Notepad. You may read or print the file. If the file is too big to view in Notepad, you may have to stop the DNS server and open the file in Wordpad.

Viewing DNS server statistics

DNS server statistics can help you determine the work load and performance of your DNS server. DNS server statistics summarize the number of queries the server received and the number of replies it sent since the last time the server restarted its database. You must start the DNS server in order to view statistics.

To view DNS server statistics, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Expand **DNS Server —> Primary Domains** and select the primary domain you want to view.
4. Click the **Statistics** icon in the toolbar.

For more information about server statistics, see Understanding DNS server statistics.

Understanding DNS server statistics

DNS server statistics summarize the number of query hits the server received and output packets it sent since the last time the server restarted or reloaded its database.

You can use this statistics information as a debugging and monitoring tool to help determine the level of query activity your name server handles. Looking at the server statistics should be the first thing you do if you suspect that you have a DNS configuration problem. The statistics information can help you determine:

- How busy the name server is. For example, you can find the number of queries your name server receives per second by dividing the total number of queries received by the total number of seconds your name server has been running (time since restart).
- Which hosts are sending the most queries to the name server. For each host, you can tell if the number and type of queries sent to the name server appear appropriate. If some hosts appear to be making a large (or unnecessary) number of a certain type of query, you may need to change your DNS configuration. You may also need, at some point, to consider adding a name server to balance the query load.

You generally should monitor your name server statistics frequently in order to understand the kind of statistics information that is normal for your DNS configuration. The statistics you get depend on whether the name server is primary, secondary, or cache-only. The statistics also depend on where in the domain structure the name server resides.

Information is continually appended to this file until you delete it. Delete the file as often as your network configuration requires. If you need to delete the file, you can find it through AS/400 Operations Navigator. (Read how to access AS/400 Operations Navigator.) The file name is STATISTICS in your AS/400 directory path:

FileSystems\Root\QIBM\UserData\OS400\DNS

You can more easily read the statistics information if you understand its basic format. There are essentially two sections. The first section contains general information about the name server. The second section contains query information about the hosts with which the name server has exchanged packets.

DNS server section

The name server section includes information about:

- The time in seconds that the name server has been running since it last started.
- The time in seconds that the name server has been running since it last refreshed its database. Typically, the time since it restarted and the time since it last refreshed its database are the same if the name server is a secondary server. If the times are different, the name server is generally a master name server for some domain.
- The number of responses the name server has received for each resource record type since it last restarted or refreshed its database. Typically, the most common resource record types are **A**, **PTR**, and **MX**.

Here is a brief description of common resource record types for DNS server section:

A	Queries for mapping host names to IP addresses.
ANY	Queries for data of any type for a host name.
AXFER	Queries for a zone transfer. Secondary servers initiate this resource record type.
CNAME	Queries an alias that points to the host’s official host name.
HINFO	Queries for host-specified information such as the CPU type and operating system.
MX	Queries for electronic mail-related information. Mail exchangers initiate this resource record type.
NS	Queries domain name servers.
PTR	Queries for mapping IP addresses to host names.
SOA	Queries for Start of Authority (SOA). Secondary servers initiate this resource record type to see if their data is current.
TXT	Queries for return of a text string. One use of this resource record type might be to identify the location of your host.
WKS	Queries for well-known services that are provided by a particular protocol on a particular interface.

Host section

The host section includes detailed information about each host with which the name server has exchanged packets since the name server last restarted or refreshed its database. The IP address for each host is followed by information about that host displayed in columns on the next line.

The information about each host corresponds with the legend that displays before the host addresses, though each column is not specifically labeled with a heading or title.

Here is an explanation of each column:

RQ	Indicates the number of queries received from this host.
RR	Indicates the number of responses received from this host.
RIQ	Indicates the number of inverse queries received from this host.
RNXD	Indicates the number of ″no such domain″ answers received from this host.
RFwdQ	Indicates the number of queries from this host that need additional processing before they can be answered.
RFwdR	Indicates the number of responses received from this host that answered the original query and were passed back to the application that made the query.
RDupQ	Indicates the number of duplicate queries from this host.
RDupR	Indicates the number of duplicate responses from this host.
RFail	Indicates the number of SERVFAIL responses. A SERVFAIL response indicates a server failure.
RFErr	Indicates the number of FORMERR responses from this host. A FORMERR means that the remote name server indicated that the local name server's query had a format error.
RErr	Indicates the number of errors that were not either SERVFAIL or FORMERR.
RTCP	Indicates the number of queries received on TCP connections from this host.
RAXFR	Indicates the number of zone transfers initiated.
RLame	Indicates the number of lame delegations received.
ROpts	Indicates the number of packets received with IP options.
SSysQ	Indicates the number of system queries sent to this host.
SAns	Indicates the number of answers sent to this host.
SFwdQ	Indicates the number of queries forwarded to this host when the answer was not in this name server's domain data or cache.
SFwdR	Indicates the number of responses from some name server that were forwarded to this host.
SDupQ	Indicates the number of duplicate queries sent to this host.
SFail	Indicates the number of SERVFAIL responses sent to this host.
SFErr	Indicates the number of FORMERR responses sent to this host.
SErr	Indicates the number of sendto() system calls that failed when the destination was this host.

RNotNsQ	Indicates the number of queries received that were not from name servers. SNaAns - Indicates the number of non-authoritative answers sent to this host.
SNXD	Indicates the number of ″no such domain″ answers sent to this host.

The host section has a Global entry for hosts as well as individual entries for each host. The Global entry totals all the statistical information in each column for all the hosts in the list. The totals in the Global entry and the type and number of individual host entries depends on several things, including the type of the name server and the type of applications in your environment.

For more information on the contents of the statistics information and how to use it, refer to the appropriate BIND documentation.

Viewing the DNS server database dump

The DNS server database can provide useful information that might help diagnose a DNS server problem, or to determine that the DNS server is performing correctly. You must start the DNS server in order to view the database dump.

Operations Navigator’s database dump is a combination of information from several sources, including:

- The contents of the DNS server’s primary and secondary domains.
- The contents of the DNS server cache database file (where root server addresses are stored).
- The DNS server’s cached query responses.

To view DNS server database dump, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Expand **DNS Server —> Primary Domains** and select the primary domain you want to view.
4. Click the **Database** icon in the toolbar.

For more information about the database dump, see Understanding the DNS server database dump.

Understanding the DNS server database dump

The DNS server database dump displays the contents of the name server cache, which is a dump of the DNS database for this server.

You can use the database dump as a debugging tool to determine whether DNS is resolving IP addresses to host names correctly. You can match the contents of the database dump to the contents of a particular host’s property pages. The database dump includes the name server’s authoritative data and cache data, as well as information about its root servers.

Comment fields divide the dump information into major sections:

Look first for **;---Cache & Data**. This is the start of the section that describes the name server’s authoritative data and cache data.

The other major section is **; ---Hints ---**. This is the start of the section that describes the name server's root servers.

Look next for the information records associated with each domain. The start of each domain's entries are identified by this record identifier: **$ORIGIN**, followed by the name of the domain. All entries in the dump are grouped by domain.

The records following the $ORIGIN <domain name> record have this general format, even though there are no column headings labeled as such:

<domain name> <TTL> <CLASS> <TYPE> <RDATA>

Where:

<domain name>	Specifies the domain name relative to the domain name in $ORIGIN. You can tell what the fully qualified domain name is by appending the domain name after the $ORIGIN to this domain name.
<TTL>	Specifies the time to live (TTL) value for this domain entry. This is the time interval in seconds that this entry may be put into the cache before the name server discards it.
<CLASS>	Specifies the record class for this domain entry. This value is always IN, which represents the Internet class.
<TYPE>	Specifies the type of resource record for this domain entry. This represents the type of query that the name server handled. The types of resource records include **A**, **PTR**, **NS**, **MX**, and so on. Entries with a resource record of type **A** may be the most common ones you look at because those resolve host names to IP addresses. The next most useful types are **NS** (which identifies other name servers), **PTR** (which resolves IP addresses to host names), and **MX** (which resolves mail exchanger queries).
<RDATA>	Specifies the resource record data for this domain entry. The actual data you see in your dump depends on the class and type of the entry. Each domain entry is usually followed by one or more tags. See the next table for the tags.

For **<RDATA>**, the most common tags are:

;NT	Specifies that this is an address record of a name server. The number following **;NT** represents the length of time it has taken to get information from a name server. The name server stores the NT value so that it knows which name servers have responded most quickly. The name server selects the name server with the lowest time first.
;CL	Specifies that this is an address record for either authoritative data or a root server. The number following **;CL** is a value identifying the hierarchy of the domain level within the domain name space. For example, if your domain is mycompany.com, then mycompany is level 2, com is level 1, and the root is level 0.
;CR	Specifies that this is an address record for a cache entry. The number following **;CR** is an identifier of how credible the data is.
auth	Specifies that the authoritative bit for this data is set on. This means that the name server received the data from a name server that was authoritative for the data sent. The data is from the answer section of the packet that was sent in response.

answer	Specifies that the authoritative bit for this data is set off. This means that the name server received the data from a name server that was not authoritative for the data sent. The data sent was in the remote name server's cache. The data is from the answer section of the response packet.
addtnl	Specifies that the data is from a section of the response packet other than the answer section. For more information on the contents of the cache dump and how to use it, refer to the appropriate BIND documentation.

Backing up DNS configuration files and maintaining log files

AS/400 Operations Navigator creates and stores DNS server and domain configuration files, and domain database files, in this directory:

```
File Systems/Integrated
File Systems/Root/QIBM/UserData/OS400/DNS
```

You should back up these configuration and database files:

- BOOT
- CACHE
- All forward mapping domain files. Example: `MYCOMPANY.MYDOMAIN.COM.DB`
- All reverse mapping domain files. Example: `3.2.1.IN-ADDR.ARPA.DB`

The following files also reside in the DNS directory, but do not need to be backed up. Log files can grow very large and they should be deleted on a regular basis. All DNS server log file contents are cleared when the DNS server is stopped and started.

- QUERYLOG. The DNS server log of queries received. The file is created when the DNS server log is active. When active, this file can grow very large and it should be deleted on a regular basis.
- DUMPDB. The DNS server database dump file. Click **Database** to create this file.
- STATISTICS. The DNS server statistics log file. Click the icon to create or append this file.
- RUNDEBUG. The DNS server debug log file. This file is created when the DNS debug function is active. When active, this file can grow very large and it should be deleted on a regular basis.
- PID. This file is created each time the DNS server is started. It is used for the Database, Statistics, and Update server functions. Do not delete or edit this file.

Files in the DNS/TMP directory

The DNS server creates temporary files as needed in `File Systems/Integrated File Systems/Root/Qibm/UserData/OS400/DNS/TMP`. These temporary files do not require any mair

Local host table versus domain name server

A local host table is a source of addressing information. The local host table provides a simple lookup on a recipient's host name that gives the Internet address of that host. If your host does not have a domain name server, the local host table is the only source for SMTP addressing.

SMTP can check the local host table for recipient addresses either before or after checking the domain name servers. The search order is based on what order you specify: search host table first or search name server first. Other applications use the resolver which does check the host table even if the domain name server is searched first.

Address resolution by way of a domain name server is not necessarily preferable over resolution by way of the local host table. IBM recommends careful use of both. A significant limitation of the local host table is its lack of ability to identify the mail exchanger for a host.

The default is to search DNS first but this may not be what is needed, depending on your configuration.

The local host table and the DNS can in fact be used together. SMTP needs information in the local host table in some scenarios. The local host table is a place for overrides. If it is *not* searched first, SMTP will often not see these overrides. While searching the local host tables first does not preclude using DNS to find results, the *reverse* is sometimes true. Note that the local host table can be both faster and more reliable if the domain name server is not available due to network problems.

Domain name servers fulfill these functions:

- Maintain MX resource data
- Build addressing information dynamically
- Exchange information with other name servers
- Contact other name servers on behalf of the requester
- Refer the requester to a server with more authority

Note: The AS/400 resolver to the domain name server maintains a cache of authoritative name server responses. This makes it unnecessary for an AS/400 to query the name server each time SMTP needs to resolve an address for a recipient. When the requested data is in the AS/400 resolver cache, the AS/400 resolver returns cached resource records to the SMTP program without any Internet traffic. The AS/400 resolver deletes the cached resource data when the time-to-live value has expired. The system keeps the local cache current on a schedule that the domain name server dictates. The AS/400 resolver does not support all SMTP queries.

Chapter 8. Troubleshooting DNS servers

Once you have created your servers, you need to activate them and verify that they are working. You can then configure your AS/400 to use your servers. You can track and verify that your DNS server on AS/400 is functioning properly by using a variety of logs, statistics, and debug features. The DNS debug function can also provide useful information that may help you troubleshoot and correct DNS server problems.

For more information on identifying problems with DNS, refer to Determining Problems for DNS Server (Chapter 21.9) in the OS/400 TCP/IP Configuration and Reference book.

For what you need to know about troubleshooting DNS servers, see:

- Setting the DNS debug level: The DNS debug function can provide useful information that may help you determine and correct DNS server problems.
- Changing the debug level: It is possible to change the DNS server debug level without stopping and restarting the DNS server. This is helpful in cases when you do not want to lose the contents of the debug file.
- Viewing the DNS debug log.

Setting the DNS server debug level

The DNS debug function can provide useful information that may help you determine and correct DNS server problems. Debug information is written to the RUNDEBUG file in the DNS directory.

Note: Your AS/400 user profile must have System Configuration (*IOSYSCFG) special authority to change the debug level. See Granting DNS authority for information about granting this authority to your user profile.

Recommendations for using DNS debug

- Keep the debug level set to 0 during normal DNS server operation. Under normal DNS server operation, leave the debug level set to 0, which is the default value. A debug level of 0 is the same as turning debug information off.
- Only use debug to diagnose DNS problems.
- Return the debug level to 0 as soon as the DNS problem is solved.
- Delete the debug log file as soon as the DNS problem is solved.

Debug values

Valid values for debug level are 1 through 11. Your IBM service representative can help you determine the appropriate debug value for diagnosing your DNS problem. Values of 1 or higher write debug information to this file:

```
/QIBM/UserData/OS400/DNS/RUNDEBUG
```

Debug log file

The RUNDEBUG debug file continues to grow as long as the debug level is set to 1 or higher, and the DNS server continues to run. It is a good idea to delete the file from time to time to keep it from taking up too much disk space. See Viewing the DNS debug log for information about accessing the file.

Notes:
1. High debug-level values increase the time it takes for the DNS server to initialize.
2. Changes to the debug value do not take effect until the DNS server is restarted. To change the debug level without stopping and restarting the DNS server, see Changing the debug level.
3. The debug log file is rewritten each time the DNS server is started, when debug is set to a level of 1 or higher.

You can set the debug level with AS/400 Operations Navigator or with the command line.

To set the DNS debug level with Operations Navigator, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> Network —> Servers —> TCP/IP**.
2. In the right pane, double-click **DNS** to open the DNS Server Configuration window.
3. Right-click **DNS Server** and select **Properties**.
4. Select the **General** tab.
5. Set the **Debug level** to a value between 1 and 11. (To turn Debug level off, set **Debug level** to **0**.)
6. Click **OK** to close the **DNS Server Properties** dialog.
7. Right-click **DNS Server** and select **Update Server**.
8. Close the DNS Server Configuration window.
9. Click **Yes** to save configuration changes.
10. Stop then restart the DNS Server.

To set the DNS debug level with the command line, follow these steps:

Enter `CHGDNSA` at the command line and press **F1** for help.

Changing the debug level

It is possible to change the DNS server debug level without stopping and restarting the DNS server. This is helpful in cases when you do not want to lose the contents of the debug file. It is also helpful when you want to keep the server's cached queries. Using these procedures to change the debug value does not change the debug value set in Operations Navigator, or by the CHGDNSA DEBUG command. That value will be used to set the debug level when the DNS server is started.

These are AS/400 command line procedures:

Getting authority to use this program

Use this command to grant authority to use this program to your AS/400 user profile:

```
GRTOBJAUT OBJ(QDNS/QTOBDRVS) OBJTYPE(*PGM) USER(MYPROFILE) AUT(*USE)
```

Substitute the name of your user profile for MYPROFILE in the above example.

Increasing the debug value (Bump)

DNS debug has a valid value range of 0 through 11. Using 0 as the debug value is the same as turning off DNS debug. The maximum value is 11, and this value writes the greatest amount of debug information to the debug log. You may repeat the bump command as many times as necessary to reach the desired debug value. Use this command to increase the current debug value by 1:

```
CALL PGM(QDNS/QTOBDRVS) PARM(BUMP)
```

Turning debug off (reset to 0)

Use this command to turn debug off by resetting the debug value to 0:

```
CALL PGM(QDNS/QTOBDRVS)) PARM(OFF)
```

Note: Changes to the DNS debug level that are made by this program are effective immediately. Do not stop and restart the DNS server.

Viewing the DNS debug log

To view the DNS debug log in Notepad, follow these steps:

1. In Operations Navigator, expand **your AS/400 server —> File Systems —> Integrated File Systems —> Root —> QIBM —> OS400 —> DNS —> RUNDEBUG**.
2. Select **Notepad** from the list of applications.
3. Click **OK**. You may read or print the debug file. If the file is too big, stop the DNS server and open the file in Wordpad.

Chapter 9. DNS and SMTP

Domain Name System (DNS) includes information for sending electronic mail by using mail exchanger information. If the network is using DNS, an SMTP (Simple Mail Transfer Protocol) application does not simply deliver mail addressed to host TEST.IBM.COM by opening a TCP connection to TEST.IBM.COM. SMTP first queries the DNS server to find out which host servers can be used to deliver the message.

Delivering mail to a specific address

DNS servers use resource records that are known as mail exchanger (MX) records. MX records map a domain or host name to a preference value and host name. MX records are generally used to designate that one host is used to process mail for another host. The records are also used to designate another host to try to deliver mail to if the first host cannot be reached. In other words, they allow mail that is addressed to one host to be delivered to a different host.

Multiple MX resource records may exist for the same domain or host name. When multiple MX records exist for the same domain or host, the preference (or priority) value of each record determines the order in which they are tried. The lowest preference value corresponds to the most preferred record, which will be tried first. When the most preferred host cannot be reached, the sending mail application tries to contact the next, less preferred MX host. The domain administrator, or the creator of the MX record, sets the preference value.

A DNS server can respond with an empty list of MX resource records when the name is in the DNS server's authority but has no MX assigned to it. When this occurs, the sending mail application may try to establish a connection with the destination host directly.

Note: Using a wild card (example: `*.mycompany.com`) MX records for a domain is not recommended.

Example: MX record for a host

In the following example, the system should, by preference, deliver mail for fsc5.test.ibm.com to the host itself. If the host cannot be reached, the system might deliver the mail to psfred.test.ibm.com or to mvs.test.ibm.com (if psfred.test.ibm.com also cannot be reached). This is an example of what these MX records would look like:

```
fsc5.test.ibm.com   IN MX 0 fsc5.test.ibm.com
                    IN MX 2 psfred.test.ibm.com
                    IN MX 4 mvs.test.ibm.com
```

Mail exchanger records can be declared when adding hosts to a domain.

Once hosts have been created, you can add host mail exchanger records.

You may also need to refer to:

Local host table versus Domain name server

Chapter 10. DNS domain concepts

DNS divides a TCP/IP network into domains, and organizes these domains into a hierarchy that is similar to the roots of a tree. It is important to understand this hierarchy in order to make informed choices when you are performing DNS procedures. Several domains may be included in a zone. A zone defines an area of DNS responsibility. Review these topics for more information about DNS domains:

- Domains and domain names: Many DNS procedures require you to enter a fully qualified domain name.
- DNS configuration files: A DNS (Domain Name System) server uses several configuration files to load its database.
- Forward and reverse mapping primary domains: DNS stores host name and IP address information about the hosts in a domain in these two types of files.
- Zones of authority: A zone of authority defines an area of DNS responsibility that owns the DNS information about the hosts within the zone. Several domains may be included in a zone.

Domains and domain names

Many DNS procedures require you to enter a fully qualified domain name. You can also refer to fully qualified domain names as complete or absolute domain names. DNS divides a TCP/IP network into domains, and organizes these domains into a hierarchy that is similar to the roots of a tree.

Let us use the Internet to illustrate the ’rootlike’ hierarchy of DNS. At the top of the Internet DNS hierarchy is a single domain called the root. The root domain is divided into subdomains with names such as **com**, **edu**, **gov**, and **mil**. These subdomains, which one can also refer to as domains, are also divided into subdomains, each with a different name. For example, **ibm** is a subdomain of the **com** domain. The ibm domain is also divided into subdomains. Imagine that the name of one of those subdomains is **as400**.

The as400 domain’s fully qualified domain name lists all of the subdomains in the hierarchy that it is part of, up to the root domain. The root domain is not referred to by name; a dot or period represents it. The as400 domain’s fully qualified domain name would look like this:

```
as400.ibm.com.
```

fully qualified domain names list all subdomains from the local domain to the root and end with a period. A complete, or fully qualified domain name ends with a period. An incomplete, or relative domain name does not end with a period.

fully qualified host names

fully qualified host names are similar to fully qualified domain names. fully qualified host names list all subdomains from the local domain to the root. They also end with a period, and list the host’s name. Imagine that there is a host in the as400 domain that is named **host1**. The fully qualified host name of host1 would look like this:

```
host1.as400.ibm.com.
```

DNS configuration files

Operations Navigator creates, deletes, and changes DNS configuration files for you as needed when you perform DNS configuration or administration tasks. You should not edit DNS configuration files directly. Instead, use Operations Navigator to change or update the files as needed.

DNS files

A DNS server uses several files to load its database. AS/400 DNS server's configuration files, including the boot file, are kept in this Integrated File System directory:

```
/QIBM/UserData/OS400/DNS
```

The configuration files include:
- Boot
- Cache
- Forward mapping primary domain
- Reverse mapping primary domain

Boot file

The DNS server reads the boot file first when it starts up. The boot file contains records that do this:
- Define the zones for which this DNS server is authoritative.
- Identify the names of the other DNS files.

Cache file

The cache file contains the data the DNS server needs when it cannot resolve a query. When no other information is available, the root server addresses in the cache file provide the DNS server a place to start.

Forward mapping primary domain file

The forward mapping primary domain files contain all data for mapping host names to IP addresses for the machines in its zone. The boot file specifies the names of the forward mapping primary domain files. The DNS server resolves the conversion of host names to IP addresses by finding the A (address) resource record associated with a host name, such as: host1.mycompany.com.

Reverse mapping primary domain file

The reverse mapping primary domain files contain all data for mapping IP addresses to host names. The system resolves the conversion of IP addresses to host names by finding the pointer (PTR) resource record associated with the name x4.x3.x2.x1.in-addr.arpa. To determine the host name that is associated with IP address 1.2.3.4, the DNS server looks for information that is stored in the reverse mapping primary domain file associated with the entry 4.3.2.1.in-addr.arpa. Notice the unusual reverse order format of this entry.

The DNS Name Server Configuration wizard creates a special reverse mapping file: 0.0.127.IN-ADDR.ARPA.DB. This file contains the PTR record for the local loopback interface. This loopback interface, which is usually named **localhost**, has the address of 127.0.0.1. Hosts use 127.0.0.1 to direct traffic to themselves.

The boot file specifies the names of the reverse mapping primary domain files.

Note:

Resource records perform a variety of functions:

- Store IP address information and host name information.
- Identify a host’s alias names.
- Identify hosts that perform mail exchanger service for other hosts.
- Identify a zone’s authoritative DNS servers.
- Record other important pieces of DNS information.

The table below describes common DNS resource records:

Record type	Description
A	Address record. It maps a host name to an IP address.
CNAME	Canonical Name record. It maps alias names to the real name of a host.
PTR	Pointer record. It maps an IP address to host name.
MX	Mail Exchanger records. MX records identify hosts that deliver or process mail for domains or other hosts.
NS	Name Server record. NS records identify the authoritative DNS servers for other domains.
SOA	Start of Authority record. Only one SOA record is allowed in each domain. The SOA record determines the authoritative DNS server for the local domain.

Forward and reverse mapping primary domains

DNS stores host name and IP address information about the hosts in a domain in two types of files:

- Forward mapping primary domain
- Reverse mapping primary domain

Operations Navigator creates these files for you when you configure domains and primary DNS servers.

Forward mapping primary domain

The forward mapping primary domain contains the host names of the hosts in the domain, and the IP addresses that are mapped to the names. When a DNS server receives a query that contains a host name, it looks for the host name in its forward mapping primary domain file. If it finds the IP address, it returns the address to the requesting host or DNS server.

Forward mapping primary domains store host name and IP address information as DNS resource records called address records. DNS identifies address records as **A** records. An example of an A record for a host named host1 in a domain that is named as400 would appear as follows:

```
host1.as400.ibm.com.   IN A 1.2.3.4
```

Reverse mapping primary domain

Reverse mapping primary domains contain IP addresses, and the host names that are mapped to them. When a DNS server receives a query that contains an IP address, it searches its reverse mapping primary domain files for the address. If it finds the host name that is mapped to the address, it returns the host name to the requesting host or DNS server.

Reverse mapping primary domains store host name and IP address information in the form of DNS resource records called pointer records. DNS identifies pointer records as **PTR** records. A PTR record for a host that is named host1, with an IP address of 1.2.3.4, in a domain that is named as400.ibm.com would appear as follows:

```
4.3.2.1.in-addr.arpa.  IN  PTR host1.as400.ibm.com.
```

You may also need to refer to:

- Automatically creating reverse mapping records: Operations Navigator can create a reverse mapping primary domain record automatically when you add a forward mapping primary domain record.

Zones of authority

A zone of authority is an area of a DNS name space. A zone may contain several domains, or it may contain a part of a single domain. Most important, a zone defines an area of DNS responsibility. That responsibility means owning the DNS information about the hosts within the zone. For every zone, there are at least one primary domain, at least one primary DNS server, and at least one DNS administrator.

Authoritative DNS servers

When a DNS server answers a query about a host whose DNS information is kept in its primary domain files, the answer is said to be **authoritative**. A DNS server is authoritative for the hosts in a primary domain if it gets its domain data from a zone's primary domain files. If a secondary DNS server loads its DNS data from a primary DNS server's domain files, the secondary DNS server is also authoritative for that zone.

SOA records

The Start of Authority (SOA) record identifies the DNS server that has authority for the domain. Operations Navigator creates this record for you when you configure a Primary DNS server or a Primary Domain.

Chapter 11. Other information about DNS

For additional information about DNS, refer to the following documents:

- OS/400 TCP/IP Configuration and Reference .
- AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support .
- AS/400 Tips and Tools for Securing Your AS/400 contains DNS security information.
- The Global AS/400 Technical Support site offers helpful installation and configuration tips. You can search the Support Line Knowledge Base by opening the **All Documents** view and clicking **Search**, then searching for keyword *DNS*.
- Requests for Comments (RFCs) are available in many places on the web. RFCs related to DNS have been grouped together into a single page: DNS related RFCs .

Printed in U.S.A.