



System i
Networking
Domain Name System

Version 5 Release 4





System i
Networking
Domain Name System

Version 5 Release 4

Note

Before using this information and the product it supports, read the information in “Notices,” on page 37.

Sixth Edition (February 2006)

This edition applies to version 5, release 4, modification 0, of IBM i5/OS (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

© Copyright International Business Machines Corporation 1998, 2006. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Domain Name System.	1
Printable PDF	1
Domain Name System concepts	1
Understanding zones	2
Understanding Domain Name System queries	3
Domain Name System domain setup	5
Dynamic updates.	5
BIND 8 features	6
Domain Name System resource records	8
Mail and Mail Exchanger records	11
Examples: Domain Name System	12
Example: Single Domain Name System server for an intranet.	12
Example: Single Domain Name System server with Internet access.	14
Example: Domain Name System and Dynamic Host Configuration Protocol on the same System i	16
Example: Splitting Domain Name System over firewall.	18
Planning for Domain Name System	20
Determining Domain Name System authorities	20
Determining domain structure	20
Planning security measures	21
Domain Name System requirements	22
Determining if Domain Name System is installed	23
Installing Domain Name System	23
Configuring Domain Name System	23
Accessing Domain Name System in iSeries Navigator	23
Configuring name servers	23
Creating a name server instance	24
Editing Domain Name System server properties	24
Configuring zones on a name server	24
Configuring Domain Name System to receive dynamic updates	25
Importing Domain Name System files	26
Record validation	26
Accessing external Domain Name System data	26
Managing Domain Name System	27
Verifying the Domain Name System function is working	27
Managing security keys	28
Managing Domain Name System keys	28
Managing dynamic update keys	28
Accessing Domain Name System server statistics	28
Accessing server statistics	29
Accessing an active server database	29
Maintaining Domain Name System configuration files	29
Advanced Domain Name System features	32
Changing Domain Name System attributes.	32
Starting or stopping Domain Name System servers	32
Changing debug values	32
Troubleshooting Domain Name System	33
Logging Domain Name System server messages	33
Changing Domain Name System debug settings	35
Related information for Domain Name System	35
Appendix. Notices.	37
Programming Interface Information	38
Trademarks	39
Terms and conditions	39

Domain Name System

Domain Name System (DNS) is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses.

Using DNS means that people can use simple names, such as www.jkltoys.com to locate a host, rather than using the IP address (xxx.xxx.xxx.xxx). A single server might only be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all domain names to their IP addresses. DNS servers working together is what allows computers to communicate across the Internet.

For IBM® OS/400® Version 5 Release 1 (V5R1), DNS services are based on the industry-standard DNS implementation, known as Berkeley Internet Name Domain (BIND) version 8. Previous IBM OS/400 DNS services were based on BIND version 4.9.3. To use the new BIND version 8 DNS server, you must have i5/OS® option 31 (DNS) and option 33 (PASE) installed on your IBM System i™ model. If you do not have PASE installed, you can still run the same DNS server based on BIND version 4.9.3 that was available in previous releases. However, the migration to BIND 8 provides improved functions and incorporates better security for your DNS server.

Note: This topic discusses new features based on BIND 8. If you are not using PASE to run DNS based on BIND 8, see the V4R5 DNS book for information regarding DNS based on BIND 4.9.3.

Printable PDF

Use this to view and print a PDF of this information.


- | To view or download the PDF version of this document, select [Domain Name System](#) (about 625 KB).

Saving PDF files

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

1. Right-click the PDF in your browser (right-click the link above).
- | 2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

- | You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

Domain Name System concepts

Domain Name System (DNS) is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS means that people can use simple names, such as www.jkltoys.com, to locate a host, rather than using the IP address (xxx.xxx.xxx.xxx).

A single server might only be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all domain names to their IP addresses. DNS servers working together is what allows computers to communicate across the Internet.

DNS data is broken up into a hierarchy of domains. Servers are responsible to know only a small portion of data, such as a single subdomain. The portion of a domain for which the server is directly responsible is called a zone. A DNS server that has complete host information and data for a zone is authoritative for the zone. An authoritative server can answer queries about hosts in its zone, using its own resource records. The query process depends on a number of factors. Understanding DNS queries explains the paths a client can use to resolve a query.

Understanding zones

Domain Name System (DNS) data is divided into manageable sets of data called *zones*. And each of these sets is a specific zone type.

Zones contain name and IP address information about one or more parts of a DNS domain. A server that contains all of the information for a zone is the authoritative server for the domain. Sometimes it makes sense to delegate the authority for answering DNS queries for a particular subdomain to another DNS server. In this case, the DNS server for the domain can be configured to refer the subdomain queries to the appropriate server.

For backup and redundancy, zone data is often stored on servers other than the authoritative DNS server. These other servers are called secondary servers, which load zone data from the authoritative server. Configuring secondary servers allows you to balance the demand on servers and also provides a backup in case the primary server goes down. Secondary servers obtain zone data by doing zone transfers from the authoritative server. When a secondary server is initialized, it loads a complete copy of the zone data from the primary server. The secondary server also reloads zone data from the primary server or from other secondaries for that domain when zone data changes.

DNS zone types

You can use i5/OS DNS to define several types of zones to help you manage DNS data:

Primary zone

Primary zone loads zone data directly from a file on a host. It can contain a subzone, or child zone. It can also contain resource records, such as host, alias (CNAME), address (A), or reverse mapping pointer (PTR) records.

Note: Primary zones are sometimes referred to as *master zones* in other BIND documentation.

Subzone

A subzone defines a zone within the primary zone. Subzones allow you to organize zone data into manageable pieces.

Child zone

A child zone defines a subzone and delegates responsibility for the subzone data to one or more name servers.

Alias (CNAME)

An alias defines an alternate name for a primary domain name.

Host A host object maps A and PTR records to a host. Additional resource records can be associated with a host.

Secondary zone

Secondary zone loads zone data from a zone's primary server or another secondary server. It maintains a complete copy of the zone for which it is a secondary.

Stub zone

A stub zone is similar to a secondary zone, but it only transfers the name server (NS) records for that zone.

Forward zone

A forward zone directs all queries for that particular zone to other servers.

Related concepts

“Understanding Domain Name System queries”

Domain Name System (DNS) can resolve queries on behalf of clients.

Related tasks

“Configuring zones on a name server” on page 24

After you configure a Domain Name System (DNS) server instance, you need to configure the zones for the name server.

Related reference

“Example: Single Domain Name System server for an intranet” on page 12

This example depicts a simple subnet with a Domain Name System (DNS) server for internal use.

“Domain Name System resource records” on page 8

Resource records are used to store data about domain names and IP addresses. This topic contains a searchable list of resource records supported for the i5/OS operating system.

Understanding Domain Name System queries

Domain Name System (DNS) can resolve queries on behalf of clients.

Clients use DNS servers to find information for them. The request might come directly from the client, or from an application running on the client. The client sends a query message to the DNS server that contains a fully qualified domain name (FQDN), a query type, such as a particular resource record the client requires, and the class for the domain name, which is typically the Internet (IN) class. The following figure depicts the sample network from the Single DNS server with Internet access example.

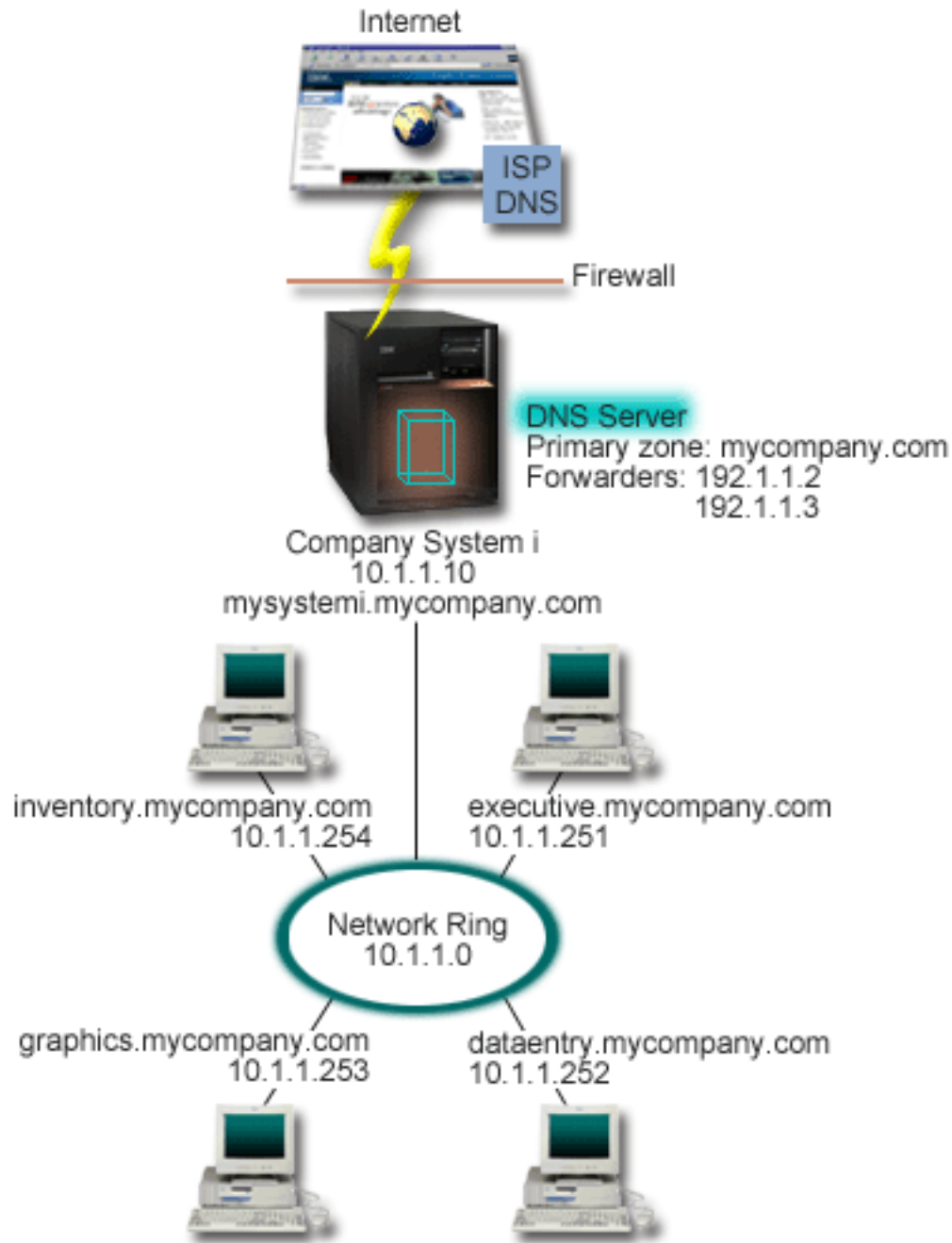


Figure 1. Single DNS server with Internet access

Suppose that host *dataentry* queries the DNS server for *graphics.mycompany.com*. The DNS server uses its own zone data and responds with the IP address 10.1.1.253.

Now suppose *dataentry* requests the IP address of *www.jkl.com*. This host is not in the DNS server's zone data. There are now two paths that can be followed, recursion or iteration. If a DNS server is set to use recursion, the server can query or contact other DNS servers on behalf of the requesting client to fully resolve the name, then send an answer back to the client. If the DNS server queries another DNS server, the requesting server will cache the answer, so it can use it the next time that it receives that query. A client can attempt to contact other DNS servers on its own behalf to resolve a name. In the process called *iteration*, the client uses separate and additional queries based on referral answers from servers.

Related reference

“Understanding zones” on page 2

Domain Name System (DNS) data is divided into manageable sets of data called *zones*. And each of these sets is a specific zone type.

“Example: Single Domain Name System server with Internet access” on page 14

This example depicts a simple subnet with a Domain Name System (DNS) server connected directly to the Internet.

Domain Name System domain setup

Domain Name System (DNS) domain setup requires domain name registration to prevent others from using your domain name.

DNS allows you to serve names and addresses on an intranet, or internal network. It also allows you to serve names and addresses to the rest of the world through the Internet. If you want to set up domains on the Internet, you are required to register a domain name.

If you are setting up an intranet, you are not required to register a domain name for internal use. Whether to register an intranet name depends on whether you want to ensure that no one else can ever use the name on the Internet, independent of your internal use. Registering a name that you are going to use internally ensures that you will never have a conflict if you later want to use the domain name externally.

Domain registration can be performed by direct contact with an authorized domain name registrar, or through some Internet Service Providers (ISPs). Some ISPs offer a service to submit domain name registration requests on your behalf. The Internet Network Information Center (InterNIC) maintains a directory of all domain name registrars that are authorized by the Internet Corporation for Assigned Names and Numbers (ICANN).

Related reference

“Example: Single Domain Name System server with Internet access” on page 14

This example depicts a simple subnet with a Domain Name System (DNS) server connected directly to the Internet.

Related information



[Internet Network Information Center \(InterNIC\)](#)

Dynamic updates

i5/OS Domain Name System (DNS) based on BIND 8 supports dynamic updates. These allow outside sources, such as Dynamic Host Configuration Protocol (DHCP), to send updates to the DNS server. In addition, you can also use DNS client tools to perform dynamic updates.

DHCP is a TCP/IP standard that uses a central server to manage IP addresses and other configuration details for an entire network. A DHCP server responds to requests from clients, dynamically assigning properties to them. DHCP allows you to define network host configuration parameters at a central location and automate the configuration of hosts. It is often used to assign temporary IP addresses to clients for networks that contain more clients than the number of IP addresses available.

In the past, all DNS data was stored in static databases. All DNS resource records had to be created and maintained by the administrator. Now, DNS servers running BIND 8 can be configured to accept requests from other sources to update zone data dynamically.

You can configure your DHCP server to send update requests to the DNS server each time it assigns a new address to a host. This automated process reduces DNS server administration in rapidly growing or changing TCP/IP networks, and in networks where hosts change locations frequently. When a client

using DHCP receives an IP address, that data is immediately sent to the DNS server. Using this method, DNS can continue to successfully resolve queries for hosts, even when their IP addresses change.

You can configure DHCP to update address mapping (A) records, reverse-lookup pointer (PTR) records, or both on behalf of a client. The A record maps a machine's host name to its IP address. The PTR record maps a machine's IP address to its host name. When a client's address changes, DHCP can automatically send an update to the DNS server so other hosts in the network can locate the client through DNS queries at its new IP address. For each record that is updated dynamically, an associated Text (TXT) record is written to identify that the record was written by DHCP.

Note: If you set DHCP to update only PTR records, you must configure DNS to allow updates from clients so that every client can update its A record. Not all DHCP clients support making their own A record update requests. Consult the documentation for your client platform before choosing this method.

Dynamic zones are secured by creating a list of authorized sources that are allowed to send updates. You can define authorized sources using individual IP addresses, whole subnets, packets that have been signed using a shared secret key (called a *Transaction Signature*, or TSIG), or any combination of those methods. DNS verifies that incoming request packets are coming from an authorized source before updating the resource records.

Dynamic updates can be performed between DNS and DHCP on a single System i model, between different System i models, or between a System i model and other systems that are capable of dynamic updates.

Note: The dynamic update application programming interface (API) QTOBUPT is required on servers that are sending dynamic updates to DNS. It is installed automatically with i5/OS Option 31, DNS.

Related concepts

Dynamic Host Configuration Protocol

Related tasks

"Configuring Domain Name System to receive dynamic updates" on page 25

Domain Name System (DNS) servers running BIND 8 can be configured to accept requests from other sources to update zone data dynamically. This topic provides instructions for configuring the allow-update option so DNS can receive dynamic updates.

Configuring the DHCP to send dynamic updates to DNS

Related reference

"Example: Domain Name System and Dynamic Host Configuration Protocol on the same System i" on page 16

This example depicts Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) on the same System i model.

"Domain Name System resource records" on page 8

Resource records are used to store data about domain names and IP addresses. This topic contains a searchable list of resource records supported for the i5/OS operating system.

QTOBUPT

"BIND 8 features"

Besides dynamic updates, BIND 8 offers several features to enhance performance of your Domain Name System (DNS) server.

BIND 8 features

Besides dynamic updates, BIND 8 offers several features to enhance performance of your Domain Name System (DNS) server.

DNS has been redesigned to use BIND 8 for i5/OS. If you do not have PASE installed, you can continue to configure and run the previously released OS/400 DNS server based on BIND 4.9.3. The DNS system requirements topic explains what you need to run BIND 8 DNS on your System i model. Using the new DNS allows you to take advantage of the following features:

Multiple DNS servers running on a single System i

In previous releases, only one DNS server can be configured. Now you can configure multiple DNS servers, or instances. This allows you to set up logical division between servers. When you create multiple instances, you must explicitly define the listen-on interface IP addresses for each one. Two DNS instances cannot listen on the same interface.

One practical application of multiple servers is split DNS, where one server is authoritative for an internal network, and a second server is used for external queries.

Conditional forwarding

Conditional forwarding allows you to configure your DNS server to fine-tune your forwarding preferences. You can set a server to forward all queries for which it does not know the answer. You can set forwarding at a global level, but add exceptions to domains for which you want to force normal iterative resolution. Or, you can set normal iterative resolution at the global level, then force forwarding within certain domains.

Secure dynamic updates

Dynamic Host Configuration Protocol (DHCP) and other authorized sources can send dynamic resource record updates, using Transaction Signatures (TSIG) or source IP address authorization, or both. This reduces the need for manual updates of zone data while ensuring that only authorized sources are used for updates.

NOTIFY

When NOTIFY is turned on, the DNS NOTIFY function is activated whenever zone data is updated on the primary server. The primary server sends out a message indicating that data has changed to all known secondary servers. Secondary servers can then respond with a zone transfer request for updated zone data. This helps improve secondary server support by keeping backup zone data current.

Zone transfers (IXFR and AXFR)

In the past, whenever secondary servers needed to reload zone data, they had to load the entire data set in an All zone transfer (AXFR). BIND 8 supports a new zone transfer method: incremental zone transfer (IXFR). IXFR is a way that other servers can transfer only changed data, instead of the entire zone.

When enabled on the primary server, data changes are assigned a flag to indicate that a change has occurred. When a secondary server requests a zone update in an IXFR, the primary server will send just the new data. IXFR is especially useful when a zone is dynamically updated. This transfer reduces the traffic load by sending smaller amounts of data.

Note: Both the primary server and secondary server must be IXFR-enabled to use this feature.

Related concepts

“Domain Name System requirements” on page 22

Consider these software requirements to run Domain Name System (DNS) on your System i model.

“Dynamic updates” on page 5

i5/OS Domain Name System (DNS) based on BIND 8 supports dynamic updates. These allow outside

sources, such as Dynamic Host Configuration Protocol (DHCP), to send updates to the DNS server. In addition, you can also use DNS client tools to perform dynamic updates.

Related reference

“Example: Splitting Domain Name System over firewall” on page 18

This example depicts Domain Name System (DNS) operating over a firewall to protect internal data from the Internet, while allowing internal users to access data on the Internet.

“Planning security measures” on page 21

Domain Name System (DNS) provides security options to limit outside access to your server.

Domain Name System resource records

Resource records are used to store data about domain names and IP addresses. This topic contains a searchable list of resource records supported for the i5/OS operating system.

A DNS zone database is made up of a collection of resource records. Each resource record specifies information about a particular object. For example, address mapping (A) records map a host name to an IP address, and reverse-lookup pointer (PTR) records map an IP address to a host name. The server uses these records to answer queries for hosts in its zone. For more information, use the table to view DNS resource records.

Table 1. Resource record lookup table

Resource record	Abbreviation	Description
Address Mapping records	A	The A record specifies the IP address of this host. A records are used to resolve a query for the IP address of a specific domain name. This record type is defined in Request for Comments (RFC) 1035.
Andrew File System Database records	AFSDB	The AFSDB record specifies the AFS® or DCE address of the object. AFSDB records are used like A records to map a domain name to its AFSDB address; or to map from the domain name of a cell to authenticated name servers for that cell. This record type is defined in RFC 1183.
Canonical Name records	CNAME	The CNAME record specifies the actual domain name of this object. When DNS queries an aliased name and finds a CNAME record pointing to the canonical name, it then queries that canonical domain name. This record type is defined in RFC 1035.
Host Information records	HINFO	The HINFO record specifies general information about a host machine. Standard CPU and operating system names are defined in the Assigned Numbers RFC 1700. However, use of the standard numbers is not required. This record type is defined in RFC 1035.

Table 1. Resource record lookup table (continued)

Resource record	Abbreviation	Description
Integrated Services Digital Network records	ISDN	The ISDN record specifies the address of this object. This record maps a host name to the ISDN address. They are used only in ISDN networks. This record type is defined in RFC 1183.
IP Version 6 Address records	AAAA	The AAAA record specifies the 128-bit address of a host. AAAA records are used like A records to map a host name to its IP address. Use AAAA records to support IP version 6 addresses, which do not fit the standard A record format. This record type is defined in RFC 1886.
Location records	LOC	The LOC record specifies the physical location of network components. These records can be used by applications to evaluate network efficiency or map the physical network. This record type is defined in RFC 1876.
Mail Exchanger records	MX	The MX records defines a mail exchanger host for mail sent to this domain. These records are used by Simple Mail Transfer Protocol (SMTP) to locate hosts that processes or forwards mail for this domain, along with preference values for each mail exchanger host. Each mail exchanger host must have a corresponding host address (A) records in a valid zone. This record type is defined in RFC 1035.
Mail Group records	MG	The MG records specifies the mail group domain name. This record type is defined in RFC 1035.
Mailbox records	MB	The MB records specifies the host domain name which contains the mailbox for this object. Mail sent to the domain is directed to the host specified in the MB record. This record type is defined in RFC 1035.
Mailbox Information records	MINFO	The MINFO records specifies the mailbox that should receive messages or errors for this object. The MINFO record is more commonly used for mailing lists than for a single mailbox. This record type is defined in RFC 1035.

Table 1. Resource record lookup table (continued)

Resource record	Abbreviation	Description
Mailbox Rename records	MR	The MR records specifies a new domain name for a mailbox. Use the MR record as a forwarding entry for a user who has moved to a different mailbox. This record type is defined in RFC 1035.
Name Server records	NS	The NS record specifies an authoritative name server for this host. This record type is defined in RFC 1035.
Network Service Access Protocol records	NSAP	The NSAP record specifies the address of a NSAP resource. NSAP records are used to map domain names to NSAP addresses. This record type is defined in RFC 1706.
Public Key records	KEY	The KEY record specifies a public key that is associated with a DNS name. The key can be for a zone, a user, or a host. This record type is defined in RFC 2065.
Responsible Person records	RP	The RP record specifies the internet mail address and description of the person responsible for this zone or host. This record type is defined in RFC 1183.
Reverse-lookup Pointer records	PTR	The PTR record specifies the domain name of a host for which you want a PTR record defined. PTR records allow a host name lookup, given an IP address. This record type is defined in RFC 1035.
Route Through records	RT	The RT record specifies a host domain name that can act as a forwarder of IP packets for this host. This record type is defined in RFC 1183.
Start of Authority records	SOA	The SOA record specifies that this server is authoritative for this zone. An authoritative server is the best source for data within a zone. The SOA record contains general information about the zone and reload rules for secondary servers. There can be only one SOA record per zone. This record type is defined in RFC 1035.

Table 1. Resource record lookup table (continued)

Resource record	Abbreviation	Description
Text records	TXT	The TXT record specifies multiple strings of text, up to 255 characters long each, to be associated with a domain name. TXT records can be used along with responsible person (RP) records to provide information about who is responsible for a zone. This record type is defined in RFC 1035. TXT records are used by i5/OS DHCP for dynamic updates. The DHCP server writes an associated TXT record for each PTR and A record update that is done by the DHCP server. DHCP records have a prefix of AS400DHCP.
Well-Known Services records	WKS	The WKS record specifies the well-known services supported by the object. Most commonly, WKS records indicate whether tcp or udp or both protocols are supported for this address. This record type is defined in RFC 1035.
X.400 Address Mapping records	PX	The PX records is a pointer to X.400/RFC 822 mapping information. This record type is defined in RFC 1664.
X25 Address Mapping records	X25	The X25 record specifies the address of an X25 resource. This record maps a host name to the PSDN address. They are used only in X25 networks. This record type is defined in RFC 1183.

Related concepts

“Mail and Mail Exchanger records”

Domain Name System (DNS) supports advanced mail routing through the use of Mail and Mail Exchanger (MX) records.

Related reference

“Example: Single Domain Name System server for an intranet” on page 12

This example depicts a simple subnet with a Domain Name System (DNS) server for internal use.

“Understanding zones” on page 2

Domain Name System (DNS) data is divided into manageable sets of data called *zones*. And each of these sets is a specific zone type.

Mail and Mail Exchanger records

Domain Name System (DNS) supports advanced mail routing through the use of Mail and Mail Exchanger (MX) records.

Mail and MX records are used by mail routing programs, such as Simple Mail Transfer Protocol (SMTP). The lookup table in DNS resource records contains the types of mail records that i5/OS DNS supports.

DNS includes information for sending electronic mail by using mail exchanger information. If the network is using DNS, an SMTP application does not 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.

Deliver 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 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 might 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 is 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 might try to establish a connection with the destination host directly.

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

Example: MX record for a host

In the following example, the system, by preference, delivers 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 will 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
```

Related reference

“Domain Name System resource records” on page 8

Resource records are used to store data about domain names and IP addresses. This topic contains a searchable list of resource records supported for the i5/OS operating system.

Examples: Domain Name System

You can use these examples to understand how to use Domain Name System (DNS) in your network.

DNS is a distributed database system for managing host names and their associated IP addresses. The following examples help to explain how DNS works, and how you can use it in your network. The examples describe the setup and reasons it will be used. They also link to related concepts that you might find useful to understand the pictures.

Example: Single Domain Name System server for an intranet

This example depicts a simple subnet with a Domain Name System (DNS) server for internal use.

The following figure depicts DNS running on a System i model for an internal network. This single DNS server instance is set up to listen for queries on all interface IP addresses. The system is a primary name

server for the mycompany.com zone.

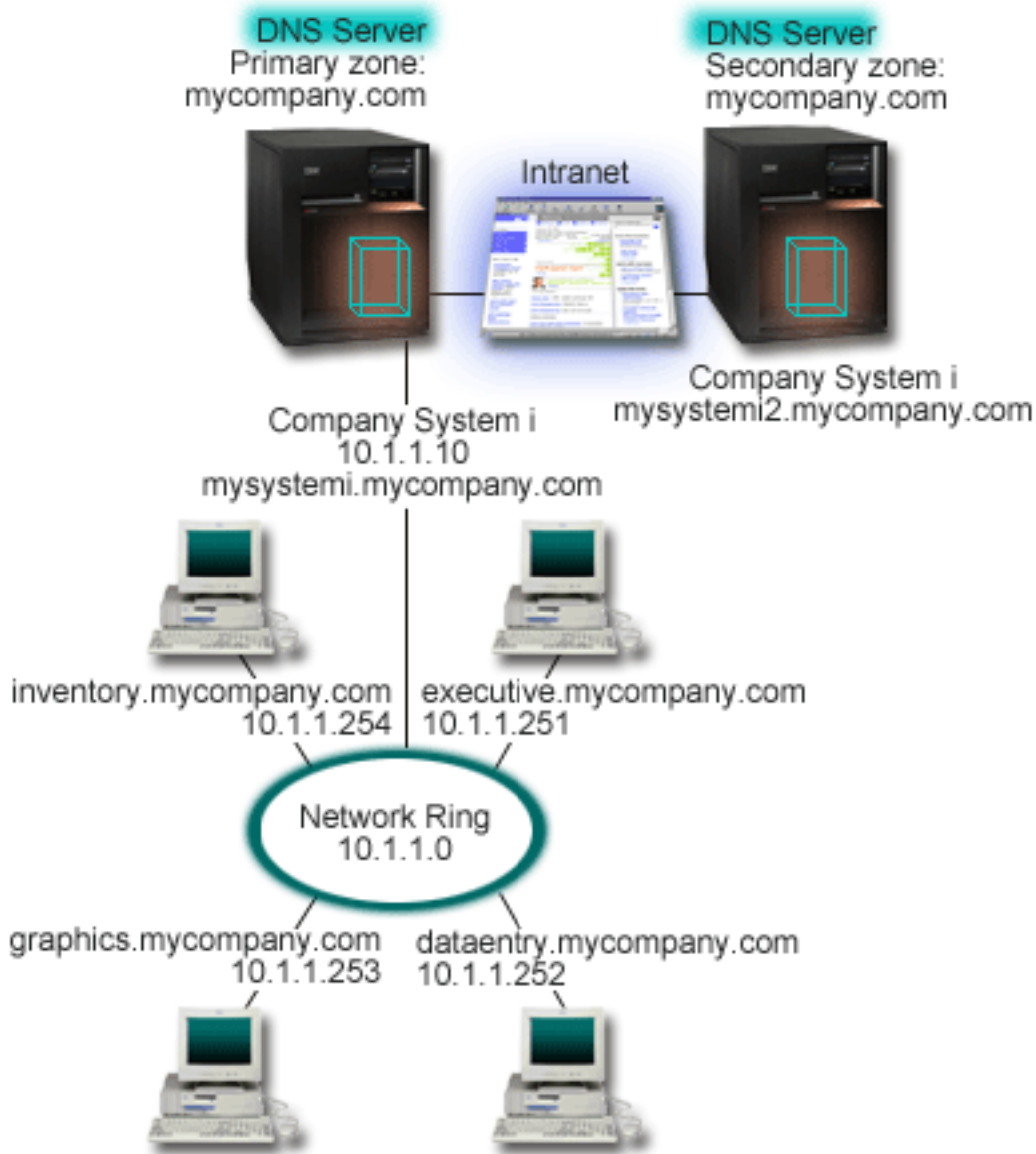


Figure 2. Single DNS server for an intranet

Each host in the zone has an IP address and a domain name. The administrator must manually define the hosts in the DNS zone data by creating resource records. Address mapping (A) records map the name of a machine to its associated IP address. This allows other hosts on the network to query the DNS server to find the IP address assigned to a particular host name. Reverse-lookup pointer (PTR) records map the IP address of a machine to its associated name. This allows other hosts on the network to query the DNS server to find the host name that corresponds to an IP address.

In addition to A and PTR records, DNS supports many other resource records that might be required, depending on what other TCP/IP based applications that you are running on your intranet. For example, if you are running internal e-mail systems, you might need to add mail exchanger (MX) records so that SMTP can query DNS to find out which systems are running the mail servers.

If this small network were part of a larger intranet, it might be necessary to define internal root servers.

Secondary servers

Secondary servers load zone data from the authoritative server. Secondary servers obtain zone data by doing zone transfers from the authoritative server. When a secondary name server starts, it requests all data for the specified domain from the primary name server. A secondary name server requests updated data from the primary server either because it receives notification from the primary name server (if the NOTIFY function is being used) or because it queries the primary name server and determines that the data has changed. In the figure above, the `mysystem1` server is part of an intranet. Another system, `mysystem2`, has been configured to act as a secondary DNS server for the `mycompany.com` zone. The secondary server can be used to balance the demand on servers and also to provide a backup in case the primary server goes down. It is a good practice to have at least one secondary server for every zone.

Related reference

“Domain Name System resource records” on page 8

Resource records are used to store data about domain names and IP addresses. This topic contains a searchable list of resource records supported for the i5/OS operating system.

“Understanding zones” on page 2

Domain Name System (DNS) data is divided into manageable sets of data called *zones*. And each of these sets is a specific zone type.

“Example: Single Domain Name System server with Internet access”

This example depicts a simple subnet with a Domain Name System (DNS) server connected directly to the Internet.

Example: Single Domain Name System server with Internet access

This example depicts a simple subnet with a Domain Name System (DNS) server connected directly to the Internet.

The following figure depicts the same example network from the single DNS server for intranet example, but now the company has added a connection to the Internet. In this example, the company is able to access the Internet, but the firewall is configured to block Internet traffic into the network.

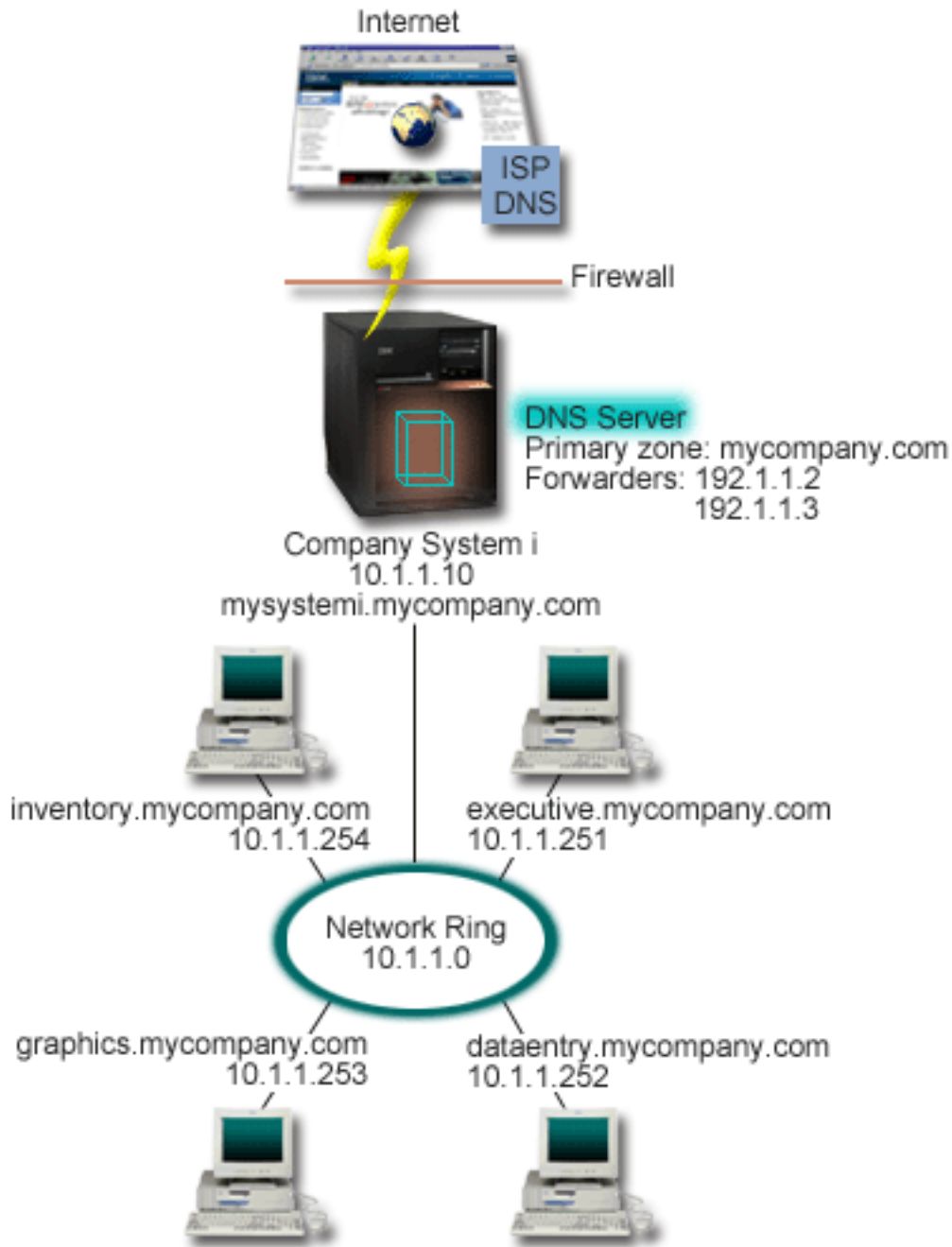


Figure 3. Single DNS server with Internet access

To resolve Internet addresses, you need to do at least one of the following tasks:

- Define Internet root servers

You can load the default Internet root servers automatically, but you might need to update the list. These servers can help to resolve addresses outside of your own zone. For instructions for obtaining the current Internet root servers, see [Accessing external Domain Name System data](#).

- Enable forwarding

You can set up forwarding to pass queries for zones outside of mycompany.com to external DNS servers, such as DNS servers run by your Internet service provider (ISP). If you want to enable

searching by both forwarding and root servers, you need to set the forward option to **first**. The server first tries forwarding and then queries the root servers only if forwarding fails to resolve the query.

The following configuration changes might also be required:

- Assign unrestricted IP addresses

In the example above, 10.x.x.x addresses are shown. However, these are restricted addresses and cannot be used outside of an intranet. They are shown below for example purposes, but your own IP addresses is determined by your ISP and other networking factors.

- Register your domain name

If you are visible to the Internet and have not already registered, you need to register a domain name.

- Establish a firewall

It is not suggested that you allow your DNS to be directly connected to the Internet. You need to configure a firewall or take other precautions to secure your System i model.

Related concepts

“Domain Name System domain setup” on page 5

Domain Name System (DNS) domain setup requires domain name registration to prevent others from using your domain name.

System i and Internet security

“Understanding Domain Name System queries” on page 3

Domain Name System (DNS) can resolve queries on behalf of clients.

Related reference

“Example: Single Domain Name System server for an intranet” on page 12

This example depicts a simple subnet with a Domain Name System (DNS) server for internal use.

Example: Domain Name System and Dynamic Host Configuration Protocol on the same System i

This example depicts Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) on the same System i model.

The configuration can be used to update DNS zone data dynamically when DHCP assigns IP addresses to hosts.

The following figure depicts a small subnet network with one System i model that acts as a DHCP and DNS server to four clients. In this work environment, suppose that the inventory, data entry, and executive clients create documents with graphics from the graphics file server. They connect to the graphics file server by a network drive to its host name.

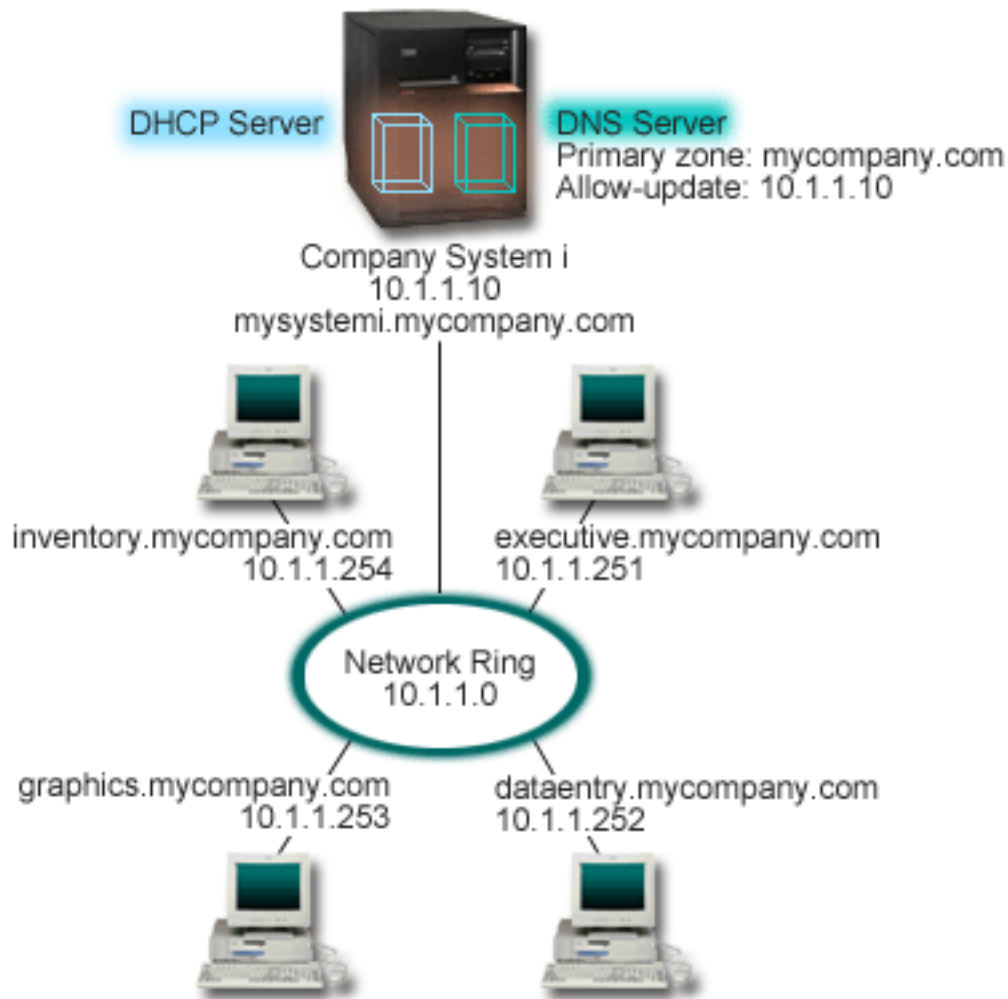


Figure 4. DNS and DHCP on the same System i model

Previous versions of DHCP and DNS were independent of each other. If DHCP assigned a new IP address to a client, the DNS records had to be manually updated by the administrator. In this example, if the graphics file server's IP address changes because it is assigned by DHCP, then its dependent clients will be unable to map a network drive to its host name because the DNS records will contain the file server's previous IP address.

With the i5/OS DNS server based on BIND 8, you can configure your DNS zone to accept dynamic updates to DNS records in conjunction with intermittent address changes through DHCP. For example, when the graphics file server renews its lease and is assigned an IP address of 10.1.1.250 by the DHCP server, the associated DNS records will be updated dynamically. This allows the other clients to query the DNS server for the graphics file server by its host name without interruption.

To configure a DNS zone to accept dynamic updates, complete the following tasks:

- Identify the dynamic zone

You cannot manually update a dynamic zone while the server is running. Doing so might cause interference with incoming dynamic updates. Manual updates can be made when the server is stopped, but you will lose any dynamic updates sent while the server is down. For this reason, you might want to configure a separate dynamic zone to minimize the need for manual updates. See Determining domain structure for more information about configuring your zones to use the dynamic update function.

- Configure the allow-update option

Any zone with the allow-update option configured is considered a dynamic zone. The allow-update option is set on a per-zone basis. To accept dynamic updates, the allow-update option must be enabled for this zone. For this example, the mycompany.com zone has allow-update data, but other zones defined on the server can be configured to be static or dynamic.

- Configure DHCP to send dynamic updates

You must authorize your DHCP server to update the DNS records for the IP addresses it has distributed.

- Configure secondary server update preferences

To keep secondary servers current, you can configure DNS to use the NOTIFY function to send a message to secondary servers for the mycompany.com zone when zone data changes. You should also configure incremental zone transfers (IXFR), which enables IXFR-enabled secondary servers to track and load only the updated zone data, instead of the entire zone.

If you run DNS and DHCP on different servers, there are some additional configuration requirements for the DHCP server.

Related concepts

“Dynamic updates” on page 5

i5/OS Domain Name System (DNS) based on BIND 8 supports dynamic updates. These allow outside sources, such as Dynamic Host Configuration Protocol (DHCP), to send updates to the DNS server. In addition, you can also use DNS client tools to perform dynamic updates.

Related tasks

Configuring the DHCP to send dynamic updates to DNS

Related reference

Example: DNS and DHCP on different System i platforms

Example: Splitting Domain Name System over firewall

This example depicts Domain Name System (DNS) operating over a firewall to protect internal data from the Internet, while allowing internal users to access data on the Internet.

The following figure depicts a simple subnet network that uses a firewall for security. With i5/OS DNS based on BIND 8, you can set up multiple DNS servers on a single System i model. Suppose that the company has an internal network with reserved IP space and an external section of a network that is available to the public.

The company wants its internal clients to be able to resolve external host names and to exchange mail with people on the outside. The company also wants its internal resolvers to have access to certain internal-only zones that are not available at all outside of the internal network. However, they do not want any outside resolvers to be able to access the internal network.

To accomplish this, the company sets up two DNS server instances on the same System i model, one for the intranet and one for everything in its public domain. This is called *split DNS*.

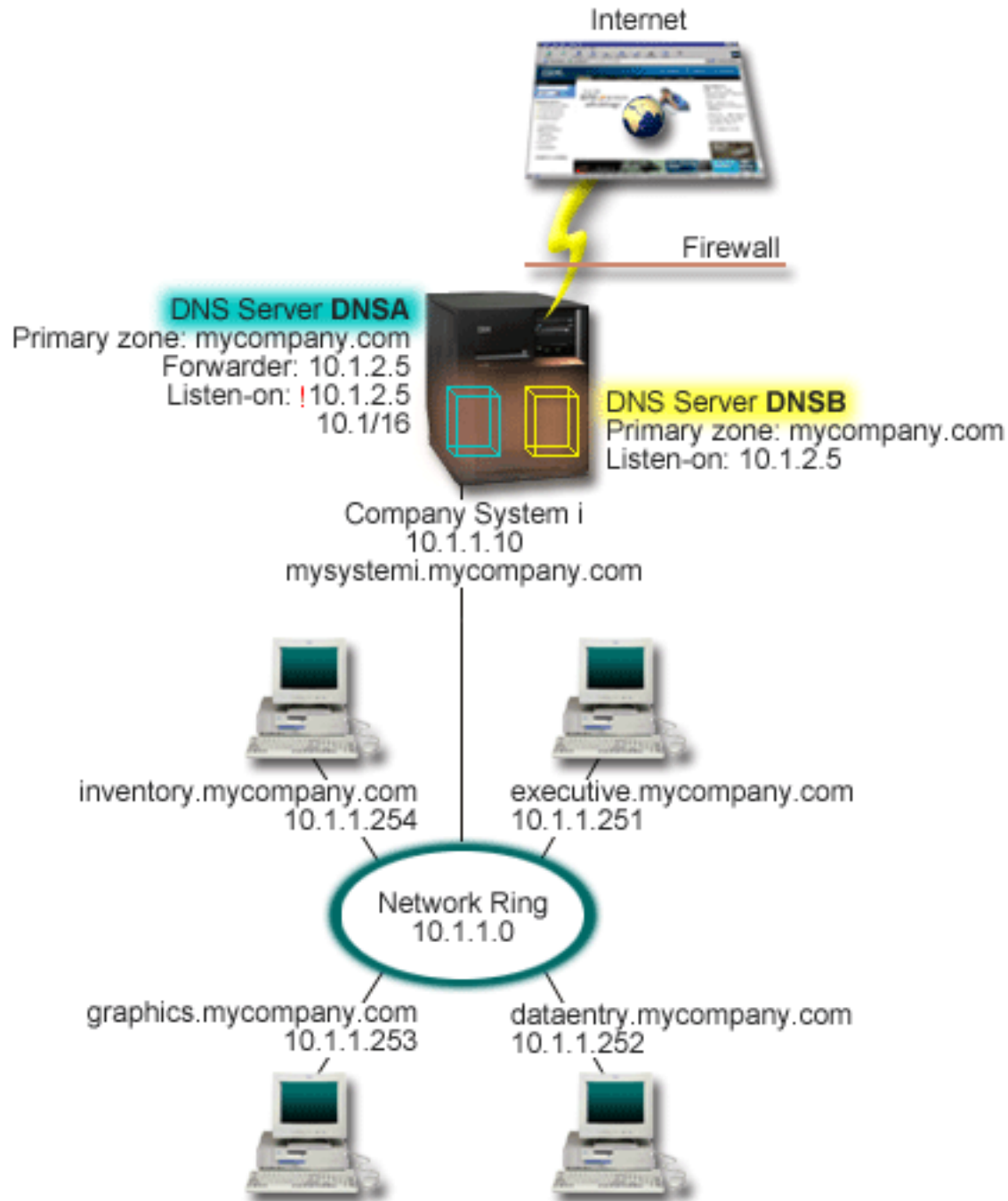


Figure 5. Split DNS over firewall

The external server, DNSB, is configured with a primary zone mycompany.com. This zone data includes only the resource records that are intended to be part of the public domain. The internal server, DNSA, is configured with a primary zone mycompany.com, but the zone data defined on DNSA contains intranet resource records. The forwarders option is defined as 10.1.2.5. This forces DNSA to forward queries it cannot resolve to the DNSB server.

If you are concerned about the integrity of your firewall or other security threats, you have the option of using the listen-on option to help protect internal data. To do this, you can configure the internal server to only allow queries to the internal mycompany.com zone from internal hosts. In order for all this to

work properly, internal clients need to be configured to query only the DNSA server. You need to consider the following configuration settings to set up split DNS:

- Listen-on

In other DNS examples, only one DNS server is on a System i model. It is set to listen on all interface IP addresses. Whenever you have multiple DNS servers on a System i model, you must define the interface IP addresses that each one listens on. Two DNS servers cannot listen on the same address. In this case, assume that all queries that come in from the firewall are sent in on 10.1.2.5. These queries should be sent to the external server. Therefore, DNSB is configured to listen on 10.1.2.5. The internal server, DNSA, is configured to accept queries from anything on the 10.1.x.x interface IP addresses except 10.1.2.5. To effectively exclude this address, the Address Match List (AML) must have the excluded address listed before the included address prefix.

- Address Match List (AML) order

The first element in the AML that a given address matches is used. For example, to allow all addresses on the 10.1.x.x network except 10.1.2.5, the ACL elements must be in the order (!10.1.2.5; 10.1/16). In this case, the address 10.1.2.5 is compared to the first element and will immediately be denied.

If the elements are reversed (10.1/16; !10.1.2.5), the IP address 10.1.2.5 will be allowed access because the server will compare it to the first element, which matches, and allow it without checking the rest of the rules.

Related reference

“BIND 8 features” on page 6

Besides dynamic updates, BIND 8 offers several features to enhance performance of your Domain Name System (DNS) server.

Planning for Domain Name System

Domain Name System (DNS) offers a variety of solutions. Before you configure DNS, it is important to plan how it works within your network. Subjects, such as network structure, performance, and security, should be assessed before you implement DNS.

Determining Domain Name System authorities

There are special authorization requirements for the Domain Name System (DNS) administrator. You should also consider security implications of authorization.

When you set up DNS, you should take security precautions to protect your configuration. You need to establish which users are authorized to make changes to the configuration.

A minimum level of authority is required to allow your administrator to configure and administer DNS. Granting all object access ensures that the administrator is capable of performing DNS administrative tasks. It is suggested that users who configure DNS have security officer access with all object (*ALLOBJ) authority. Use iSeries™ Navigator to authorize users. If you need more information, read “Granting authority to the DNS administrator” in the DNS online help.

Note: If an administrator’s profile does not have full authority, specific access and authority to all DNS directories and related configuration files must be granted.

Related reference

“Maintaining Domain Name System configuration files” on page 29

You can use i5/OS DNS to create and manage DNS server instances on your System i model. The configuration files for DNS are managed by iSeries Navigator. You must not manually edit the files. Always use iSeries Navigator to create, change, or delete DNS configuration files.

Determining domain structure

If you are setting up a domain for the first time, you should plan for demand and maintenance before creating zones.

It is important to determine how you divide your domain or subdomains into zones, how to best serve network demand, access to the Internet, and how to negotiate firewalls. These factors can be complex and must be dealt with case-by-case. Refer to authoritative sources such as the O'Reilly DNS and BIND book for in-depth guidelines.

If you configure a Domain Name System (DNS) zone as a dynamic zone, you cannot make manual changes to zone data while the server is running. Doing so might cause interference with incoming dynamic updates. If it is necessary to make manual updates, stop the server, make the changes, and then restart the server. Dynamic updates sent to a stopped DNS server will never be completed. For this reason, you might want to configure a dynamic zone and a static zone separately. You can do this by creating entirely separate zones, or by defining a new subdomain, such as `dynamic.mycompany.com`, for those clients that will be maintained dynamically.

i5/OS DNS provides a graphical interface for configuring your systems. In some cases, the interface uses terminology or concepts that might be represented differently in other sources. If you refer to other information sources when you are planning for your DNS configuration, it might be helpful to remember the following items:

- All zones and objects defined in a System i model are organized within the folders Forward Lookup Zones and Reverse Lookup Zones. Forward lookup zones are the zones that are used to map domain names to IP addresses, such as A records. The reverse lookup zones are the zones that are used to map IP addresses to domain names, such as PTR records.
- i5/OS DNS refers to *primary zones* and *secondary zones*.
- The interface uses *subzones*, which some sources refer to as *subdomains*. A child zone is a subzone for which you have delegated responsibility to one or more name servers.

Planning security measures

Domain Name System (DNS) provides security options to limit outside access to your server.

Securing your DNS server is essential. In addition to the security considerations in this topic, DNS security and System i security are covered in a variety of sources including the System i platform and the Internet topic collection. The book *DNS and BIND* also covers security related to DNS.

Address match lists

DNS uses address match lists to allow or deny outside entities access to certain DNS functions. These lists can include specific IP addresses, a subnet (using an IP prefix), or using Transaction Signature (TSIG) keys. You can define a list of entities to which you want to allow or deny access in an address match list. If you want to be able to reuse an address match list, you can save the list as an access control list (ACL). Then whenever you need to provide the list, you can call the ACL and the entire list will be loaded.

Address match list element order

The first element in an address match list that a given address matches is used. For example, to allow all addresses on the 10.1.1.x network except 10.1.1.5, the match list elements must be in the order (!10.1.1.5; 10.1.1/24). In this case, the address 10.1.1.5 will be compared to the first element and will immediately be denied.

If the elements are reversed (10.1.1/24; !10.1.1.5), the IP address 10.1.1.5 will be allowed access because the server will compare it to the first element, which matches, and allow it without checking the rest of the rules.

Access control options

DNS allows you to set limitations such as who can send dynamic updates to the server, query data, and request zone transfers. You can use ACLs to restrict access to the server for the following options:

allow-update

In order for your DNS server to accept dynamic updates from any outside sources, you must enable the allow-update option.

allow-query

Specifies which hosts are allowed to query this server. If not specified, the default is to allow queries from all hosts.

allow-transfer

Specifies which hosts are allowed to receive zone transfers from the server. If not specified, the default is to allow transfers from all hosts.

allow-recursion

Specifies which hosts are allowed to make recursive queries through this server. If not specified, the default is to allow recursive queries from all hosts.

blackhole

Specifies a list of addresses that the server does not accept queries from or use to resolve a query. Queries from these addresses will not be responded to.

Related concepts

System i and Internet security

Related reference

“BIND 8 features” on page 6

Besides dynamic updates, BIND 8 offers several features to enhance performance of your Domain Name System (DNS) server.

Domain Name System requirements

Consider these software requirements to run Domain Name System (DNS) on your System i model.

The DNS option feature, Option 31, cannot be installed automatically with the operating system. You must specifically select DNS for installation. The DNS server added for i5/OS is based on the industry-standard DNS implementation known as BIND 8. Previous OS/400 DNS services were based on BIND 4.9.3, and are still available in i5/OS.

After DNS is installed, you are by default configured to set up a single DNS server using the BIND 4.9.3-based DNS server capabilities that were available in previous releases. If you want to run one or more DNS servers using BIND 8, you must install PASE. PASE is SS1 Option 33. After PASE is installed, iSeries Navigator automatically handles configuring the correct BIND implementation.

If you do not use PASE, you will not be able to take advantage of all of the BIND 8 features. If you do not use PASE, you can still run the same DNS server based on BIND 4.9.3 that was available in previous releases. See the V4R5 DNS information center topic for BIND 4.9.3 documentation.

If you want to configure a DHCP server on a different platform to send updates to this DNS server, Option 31 must be installed on that DHCP server as well. The Dynamic Host Configuration Protocol (DHCP) server uses programming interfaces provided by Option 31 to perform dynamic updates.

Related concepts

i5/OS PASE

“Configuring Domain Name System” on page 23

You can use iSeries Navigator to configure name servers and to resolve queries outside of your domain.

Related reference

“BIND 8 features” on page 6

Besides dynamic updates, BIND 8 offers several features to enhance performance of your Domain Name System (DNS) server.

Related information



Determining if Domain Name System is installed

To determine if Domain Name System (DNS) is installed, follow these steps.

1. At the command line, type G0 LICPGM and press Enter.
2. Type 10 (Display installed licensed programs) and press Enter.
3. Page down to **5722SS1 Domain Name System** (SS1 Option 31). If DNS is installed successfully, the Installed Status will be *compatible, as shown here:

LicPgm	Installed Status	Description
5722SS1	*COMPATIBLE	Domain Name System

4. Press F3 to exit the display.

Installing Domain Name System

To install Domain Name System (DNS), follow these steps .

1. At the command line, type G0 LICPGM and press Enter.
2. Type 11 (Install licensed programs) and press Enter.
3. Type 1 (Install) in the **Option** field next to Domain Name System and press Enter.
4. Press Enter again to confirm the installation.

Configuring Domain Name System

You can use iSeries Navigator to configure name servers and to resolve queries outside of your domain.

Before you work with your Domain Name System (DNS) configuration, see DNS system requirements to install the necessary DNS components.

Related concepts

“Domain Name System requirements” on page 22

Consider these software requirements to run Domain Name System (DNS) on your System i model.

Accessing Domain Name System in iSeries Navigator

These instructions guide you to the DNS configuration interface in iSeries Navigator.

If you are using PASE, you will be able to configure DNS servers based on BIND 8. If you are not using PASE, you can still run the same DNS server based on BIND 4.9.3 that was available in previous releases. See the V4R5 DNS information center topic for information regarding DNS based on BIND 4.9.3.

If you are configuring DNS for the first time, follow these steps:

1. In iSeries Navigator, expand *your system* → **Network** → **Servers** → **DNS**.
2. Right-click **DNS** and select **New Configuration**.

Related concepts

Getting to know iSeries Navigator

Configuring name servers

Domain Name System (DNS) allows you to create multiple name server instances. This topic provides instructions for configuring a name server.

i5/OS DNS based on BIND 8 supports multiple name server instances. The following tasks guide you through the process of creating a single name server instance, including its properties and zones.

If you want to create multiple instances, repeat these procedure until all instances you want have been created. You can specify independent properties, such as debug levels and autostart values, for each name server instance. When you create a new instance, separate configuration files are created.

Related reference

“Maintaining Domain Name System configuration files” on page 29

You can use i5/OS DNS to create and manage DNS server instances on your System i model. The configuration files for DNS are managed by iSeries Navigator. You must not manually edit the files. Always use iSeries Navigator to create, change, or delete DNS configuration files.

Creating a name server instance

The New Domain Name System (DNS) Configuration wizard can help you to define a DNS server instance.

To start the **New DNS Configuration** wizard, follow these steps:

1. In **iSeries Navigator**, expand *your system* → **Network** → **Servers** → **DNS**.
2. In the left pane, right-click **DNS** and select **New Name Server...**
3. Follow the wizard’s instructions to complete the configuration process.

The wizard requires the following input:

DNS server name:

Enter a name for your DNS server. It can be up to 5 characters long and must start with an alphabetic character. If you create multiple servers, each must have a unique name. This name is referred to as the DNS server “instance” name in other areas of the system.

Listen-on IP addresses:

Two DNS servers cannot listen on the same IP address. The default setting is to listen on ALL IP addresses. If you are creating additional server instances, neither can be configured to listen on ALL. You must specify the IP addresses for each server.

Root servers:

You might load the list of default Internet root servers or specify your own root servers, such as internal root servers for an intranet.

Note: You should only consider loading the default Internet root servers if you are on the Internet and expect your DNS to be able to fully resolve Internet names.

Server start-up:

You can specify whether the server should autostart when TCP/IP is started. When you operate multiple servers, individual instances can be started and ended independently of each other.

Editing Domain Name System server properties

After you create a name server, you can edit properties such as allow-update and debug levels. These options apply only to the server instance you change.

To edit the properties of the Domain Name System (DNS) server instance, follow these steps:

1. In **iSeries Navigator**, expand *your system* → **Network** → **Servers** → **DNS**.
2. In the right pane, right-click *your DNS server* and select **Configuration**.
3. Right-click **DNS Server** and select **Properties**.

Configuring zones on a name server

After you configure a Domain Name System (DNS) server instance, you need to configure the zones for the name server.

To configure zones on your server, follow these steps:

1. In **iSeries Navigator**, expand *your system* → **Network** → **Servers** → **DNS**.

2. In the right pane, right-click *your DNS server* and select **Configuration**.
3. In the DNS Configuration window, select the zone type that you want to create by right-clicking either the **Forward Lookup Zone** or the **Reverse Lookup Zone** folder.
4. Follow the wizard's instructions to complete the creation process.

Related concepts

"Accessing external Domain Name System data" on page 26

When you create Domain Name System (DNS) zone data, your server will be able to resolve queries to that zone.

Related tasks

"Configuring Domain Name System to receive dynamic updates"

Domain Name System (DNS) servers running BIND 8 can be configured to accept requests from other sources to update zone data dynamically. This topic provides instructions for configuring the allow-update option so DNS can receive dynamic updates.

"Importing Domain Name System files" on page 26

Domain Name System (DNS) can import existing zone data files. Follow these time-saving procedures for creating a new zone from an existing configuration file.

Related reference

"Understanding zones" on page 2

Domain Name System (DNS) data is divided into manageable sets of data called *zones*. And each of these sets is a specific zone type.

Configuring Domain Name System to receive dynamic updates

Domain Name System (DNS) servers running BIND 8 can be configured to accept requests from other sources to update zone data dynamically. This topic provides instructions for configuring the allow-update option so DNS can receive dynamic updates.

When creating dynamic zones, you should consider your network structure. If parts of your domain still requires manual updates, you might want to consider setting up separate static and dynamic zones. If you need to make manual updates to a dynamic zone, you must stop the dynamic zone server and restart it after you have completed the updates. Stopping the server forces it to synchronize all dynamic updates that have been made since the server loaded its zone data from the zone database. If you do not stop the server, you will lose all dynamic updates that are processed since it is started. However, stopping the server to make manual updates means you might miss dynamic updates that are sent while the server is down.

DNS indicates that a zone is dynamic when objects are defined in the allow-update statement. To configure the allow-update option, follow these steps:

1. In iSeries Navigator, expand *your system* → **Network** → **Servers** → **DNS**.
2. In the right pane, right-click *your DNS server* and select **Configuration**.
3. In the DNS Configuration window, expand **Forward Lookup Zone** or **Reverse Lookup Zone**.
4. Right-click the primary zone that you want to edit and select **Properties**.
5. In the Primary Zone Properties page, click the **Options** tab.
6. On the Options page, expand **Access Control** → **allow-update**.
7. DNS uses an address match list to verify authorized updates. To add an object to the address match list, select an address match list element type and click **Add**. You can add an IP Address, IP Prefix, Access Control List, or Key.
8. When you have finished updating the address match list, click **OK** to close the Options page.

Related tasks

"Configuring zones on a name server" on page 24

After you configure a Domain Name System (DNS) server instance, you need to configure the zones for the name server.

Configuring the DHCP to send dynamic updates to DNS

Importing Domain Name System files

Domain Name System (DNS) can import existing zone data files. Follow these time-saving procedures for creating a new zone from an existing configuration file.

You can create a primary zone by importing a zone data file, or by converting existing host tables. Refer to [Converting host tables !\[\]\(3d8c13c92b853674f749aac6fa869926_img.jpg\)](#) to create zone data from a host table.

You can import any file that is a valid zone configuration file based on BIND syntax. The file should be located in an IFS directory. When imported, DNS verifies that it is a valid zone data file and adds it to the NAMED.CONF file for this server instance.

To import a zone file, follow these steps:

1. In iSeries Navigator, expand *your system* → **Network** → **Servers** → **DNS**.
2. In the right pane, double-click the DNS server instance into which you want to import the zone.
3. In the left pane, right-click **DNS server** and select **Import Zone**.
4. Follow the wizard's instructions to import the primary zone.

Related tasks

“Configuring zones on a name server” on page 24

After you configure a Domain Name System (DNS) server instance, you need to configure the zones for the name server.

Record validation

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

After the Import domain data function has finished, any records in error can be examined individually on the Other Records property page of the imported zone.

Notes:

1. Importing a large primary domain might take several minutes.
2. 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.

Accessing external Domain Name System data

When you create Domain Name System (DNS) zone data, your server will be able to resolve queries to that zone.

Root servers are critical to the function of a DNS server that is directly connected to the Internet or a large intranet. DNS servers must use root servers to answer queries about hosts other than those that are contained in their own domain files.

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

iSeries Navigator's default root servers list

You should use Internet root servers only if you have an Internet connection and you want to resolve names on the Internet if they are not resolved on your DNS server. A default list of Internet root server is supplied in iSeries Navigator. The list is current when iSeries Navigator is released. You can verify that

the default list is current by comparing it to the list on the InterNIC site. Update your configuration's root server list to keep it current.

Getting 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. Store the file in the following directory path: `Integrated File System/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE`

A DNS server behind a firewall might 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 might forward off-site queries to the firewall DNS. In this case, the firewall DNS server acts as a forwarder.

Intranet root servers

If your DNS server is part of a large intranet, you might have internal root servers. If your DNS server will not be accessing the Internet, you do not need to load the default Internet servers. However, you should add your internal root servers so that your DNS server can resolve internal addresses outside of its domain.

Related tasks

"Configuring zones on a name server" on page 24

After you configure a Domain Name System (DNS) server instance, you need to configure the zones for the name server.

Managing Domain Name System

Managing Domain Name System (DNS) includes verifying that the DNS function is working, monitoring performance, and maintaining DNS data and files.

Verifying the Domain Name System function is working

Name Server Lookup (NSLookup) is a tool that is used to query the Domain Name System (DNS) server for an IP address. This verifies that the DNS server is working.

Request the host name that is associated with the loopback IP address (127.0.0.1). It should respond with the host name (localhost). You should also query specific names that are defined in the server instance that you are trying to verify. This will confirm that the specific server instance you are testing is functioning properly.

To verify DNS function with NSLookup, follow these steps:

1. At the command line, type `NSLOOKUP DMNNAMSVR(n.n.n.n)`, where `n.n.n.n` is an address that you have configured the server instance you are testing to listen on.
2. At the command line, type `NSLOOKUP` and press Enter. This starts an NSLookup query session.
3. Type `server` followed by your server name and press Enter. For example: `server myiseries.mycompany.com`. This information displays:

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

Where `n.n.n.n` represents your DNS server's IP address.

4. 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:  myiseries.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**.

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

Note: If you need help using NSLookup, type `?` and press Enter.

Managing security keys

Security keys allow you to limit access to your Domain Name System (DNS) data.

There are two types of keys related to DNS. They each play a different role in securing your DNS configuration. The following descriptions explain how each relates to your DNS server.

Managing Domain Name System keys

The Domain Name System (DNS) keys are keys defined for BIND and used by the DNS server as part of the verification of an incoming update.

You can configure a key and assign it a name. Then, when you want to protect a DNS object, such as a dynamic zone, you can specify the key in the Address Match List.

To manage DNS keys, follow these steps:

1. In iSeries Navigator, expand *your system* → **Network** → **Servers** → **DNS**.
2. In the right pane, right-click the DNS server instance that you want to open and select **Configuration**.
3. In the DNS Configuration window, select **File** → **Manage Keys**.

Managing dynamic update keys

Dynamic update keys are used for securing dynamic updates by the Dynamic Host Configuration Protocol (DHCP) server.

These keys must be present when Domain Name System (DNS) and DHCP are on the same System i model. If DHCP is on a different System i model, you must create the same dynamic update key on each System i model to allow secure dynamic updates.

To manage dynamic update keys, follow these steps:

1. In iSeries Navigator, expand *your system* → **Network** → **Servers** → **DNS**.
2. Right-click **DNS** and select **Manage Dynamic Update Keys**.

Accessing Domain Name System server statistics

Database dump and statistics tools can help you review and manage server performance.

Domain Name System (DNS) provides several diagnostic tools. They can be used to monitor performance of your server.

Related reference

“Maintaining Domain Name System configuration files” on page 29

You can use i5/OS DNS to create and manage DNS server instances on your System i model. The

configuration files for DNS are managed by iSeries Navigator. You must not manually edit the files. Always use iSeries Navigator to create, change, or delete DNS configuration files.

Accessing server statistics

The server statistics summarize the number of queries and responses the server received since the last time the server restarted or reloaded its database.

Domain Name System (DNS) allows you to view the statistics for a server instance. Information is continually appended to this file until you delete the file. This information might be useful in evaluating how much traffic the server receives, and in tracking down problems. More information about server statistics is available in the DNS online help topic *Understanding DNS server statistics*.

To access server statistics, follow these steps:

1. In iSeries Navigator, expand *your system* → **Network** → **Servers** → **DNS**.
2. In the right pane, right-click *your DNS server* and select **Configuration**.
3. In the DNS configuration window, select **View** → **Server Statistics**.

Accessing an active server database

The active server database contains zone and host information, including some zone properties, such as start of authority (SOA) information, and through host properties, such as mail exchanger (MX) information, which might be useful in tracking down problems.

Domain Name System (DNS) allows you to view a dump of the authoritative data, cache data, and hints data for a server instance. The dump includes the information from all of the server's primary and secondary zones (forward and reverse mapping zones), as well as information that the server has obtained from queries.

You can view the active server database dump using iSeries Navigator. If you need to save a copy of the files, the database dump file name is NAMED_DUMP.DB in your i5/OS directory path: Integrated File System/Root/QIBM/UserData/OS400/DNS/<server instance>, where <server instance> is the name of the DNS server instance. More information about the active server database is available in the DNS online help topic *Understanding the DNS server database dump*.

To access the active server database dump, follow these steps:


1. In iSeries Navigator, expand *your system* → **Network** → **Servers** → **DNS**.
2. In the right pane, right-click *your DNS server* and select **Configuration**.
3. In the DNS configuration window, select **View** → **Active Server Database**.



Maintaining Domain Name System configuration files











You can use i5/OS DNS to create and manage DNS server instances on your System i model. The configuration files for DNS are managed by iSeries Navigator. You must not manually edit the files. Always use iSeries Navigator to create, change, or delete DNS configuration files.







DNS configuration files are stored in the integrated file system paths listed below.

Note: The file structure below applies to DNS running on BIND 8. If you are using DNS based on BIND

4.9.3, see *Backing up DNS configuration files and maintaining log files*  in the V4R5 DNS Information Center topic.

In the following table, files are listed in the hierarchy of paths shown. Files with a save icon  should be backed up to protect data. Files with a delete icon  should be deleted on a regular basis.

Name	Icon	Description
QIBM/UserData/OS400/DNS/		Starting point directory for DNS.
ATTRIBUTES		DNS uses this file to determine which BIND version you are using.
QIBM/UserData/OS400/DNS/ <instance-n>/		Starting point directory for a DNS instance.
ATTRIBUTES		Configuration attributes used by i5/OS DNS.
NAMED.CONF		This file contains configuration data. Used to tell the server what specific zones it is managing, where the zone files are, which zones can be dynamically updated, where its forwarding servers are, and other option settings.
BOOT.AS400BIND4		BIND 4.9.3 server configuration and policies file that is converted to the BIND 8 NAMED.CONF file for this instance. This file is created if you migrate a BIND 4.9.3 server to BIND 8. It serves as a backup for migration, and can be deleted when the BIND 8 server is working properly.
NAMED.CA		List of root servers for this server instance.
NAMED_DUMP.DB		Server data dump created for the active server database.
NAMED.STATS		Server statistics.
NAMED.PID		Holds Process ID of running server. 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.
QUERYLOG		The DNS server log of queries received. The file is created when the DNS server log is active. When active, this file becomes large and it should be deleted on a regular basis.
<zone-name-a>.DB		Zone file for a particular domain to be served by this server. Contains all of the resource records for this zone.
<zone-name-b>.DB		Zone file for a particular domain to be served by this server. Contains all of the resource records for this zone. Each zone has a separate .DB file.

Name	Icon	Description
.ixfr.		Incremental zone transfer (IXFR) files. These files are used by secondary servers to load only changed data since the last zone transfer. As updates are made, the number of IXFR files will grow. You should periodically delete the older IXFR files. Leaving files that were created within a day or two will allow most secondaries to still load IXFRs. If you delete all of the files, the secondary will request a full transfer (AXFR).
TMP		Directory used by server instance for creating temporary work files.
QIBM/UserData/OS400/DNS/TMP		Temp directory used by QTOBH2N program to create intermediate files dumped from the host table for later import using iSeries Navigator.
QIBM/UserData/OS400/DNS/_DYN/		Directory that holds files required for dynamic updates.
<key_id-name-x>._KID		File containing a BIND 8 key statement for the key_id named <key_id-name-x>.
<key_id-name-x>._DUK. <zone-name-a>		Dynamic update key required to initiate a dynamic update request to <zone-name-a> using the <key_id-name-x> key.
<key_id-name-y>._KID		File containing a BIND 8 key statement for the key_id named <key_id-name-y>.
<key_id-name-y>._DUK. <zone-name-a>		Dynamic update key required to initiate a dynamic update request to <zone-name-a> using the <key_id-name-y> key.
<key_id-name-y>._DUK. <zone-name-b>		Dynamic update key required to initiate a dynamic update request to <zone-name-b> using the <key_id-name-y> key.

Related concepts

“Determining Domain Name System authorities” on page 20

There are special authorization requirements for the Domain Name System (DNS) administrator. You should also consider security implications of authorization.

“Accessing Domain Name System server statistics” on page 28

Database dump and statistics tools can help you review and manage server performance.

Related tasks

“Configuring name servers” on page 23

Domain Name System (DNS) allows you to create multiple name server instances. This topic provides instructions for configuring a name server.

Advanced Domain Name System features

DNS in iSeries Navigator provides an interface with advanced features for configuring and managing your DNS server.

The tasks in the subtopics are provided as shortcuts for administrators who are familiar with the i5/OS graphical interface. They provide fast methods for changing server status and attributes for multiple instances at once.

Related tasks

“Changing Domain Name System debug settings” on page 35

The Domain Name System (DNS) debug function can provide information that can help you determine and correct DNS server problems.

Changing Domain Name System attributes

If the DNS interface does not allow you to change all server instance autostart and debug levels at once, you can use the character-based interface to change these settings for individual DNS server instances, or for all instances at once.

Follow these steps to use CHGDNSA:

1. At the command line, type CHGDNSA and press F4.
2. On the Change DNS Server Attributes (CHGDNSA) page, type the name of a single server instance, or *ALL, and press Enter.

The available server attribute options display:

```
Autostart server . . . . . *SAME *YES, *NO, *SAME
Debug level . . . . . *SAME 0-11, *SAME, *DFT
```

3. **Autostart** To specify that the DNS servers selected should automatically start when TCP/IP is started, type *YES. If you do not want the server to start when TCP/IP is started, type *NO. To leave the attribute at its current settings, type *SAME.

Debug level To change the debug level that the DNS servers selected should use, type a value between 0 and 11. To specify that the debug level should inherit the sever startup debug value, type *DFT. To leave the attribute at its current settings, type *SAME.

When you have entered all your preferences, press Enter to set the DNS attributes.

Starting or stopping Domain Name System servers

If the Domain Name System (DNS) interface does not allow you to start or stop multiple server instances at once, you can use the character-based interface to change these settings for multiple instances at once.

To use the character-based interface to start all DNS server instances at once, type STRTCPSVR SERVER(*DNS) DNSSVR(*ALL) at the command line. To stop all DNS servers at once, type ENDTCPSPVR SERVER(*DNS) DNSSVR(*ALL) at the command line.

Changing debug values

It is useful to change the debug level for administrators who have large zones and do not want the large amount of debug data collected when the server is first starting up and loading all of the zone data.

Domain Name System (DNS) in the iSeries Navigator interface does not allow you to change the debug level while the server is running. However, you can use the character-based interface to change the debug level while the server is running. To change the debug level using the character-based interface, follow these steps, replacing <instance> with the name of the server instance:

1. At the command line, type ADDLIBILE QDNS and press Enter.
2. Change the debug level:
 - To turn debugging on, or increase the debug level by 1, type CALL QTOBDRVS ('BUMP' '<instance>') and press Enter.
 - To turn debugging off, type CALL QTOBDRVS ('OFF' '<instance>') and press Enter.

Troubleshooting Domain Name System


Domain Name System (DNS) logging and debugging settings can help you resolve problems with your DNS server.

DNS operates much the same as other TCP/IP functions and applications. Like SMTP or FTP applications, DNS jobs run under the QSYSWRK subsystem and produce job logs under the user profile QTCP with information associated with the DNS job. If a DNS job ends, you can use the job logs to determine the cause. If the DNS server is not returning the expected responses, the job logs might contain information that can help with problem analysis.

The DNS configuration consists of several files with several different types of records in each file. Problems with the DNS server are generally the result of incorrect entries in the DNS configuration files. When a problem occurs, verify that the DNS configuration files contain the entries you expect.

Identifying jobs

If you look in the job log to verify DNS server function (using WRKACTJOB, for example), consider the following naming guidelines:

- If you are using BIND 4.9.3, the job name of the server will be QTOBDNS. For more information about debugging DNS 4.9.3, refer to Troubleshooting DNS servers .
- If you are running servers based on BIND 8, there will be a separate job for each server instance you are running. The job name is 5 fixed chars (QTOBD) followed by the instance name. For example, if you have two instances, INST1 and INST2, their job names will be QTOBDINST1 and QTOBDINST2.

Logging Domain Name System server messages

Domain Name System (DNS) provides numerous logging options that can be adjusted when you are trying to find the source of a problem. Logging provides flexibility by offering various severity levels, message categories, and output files so that you can fine-tune logging to help you find problems.

BIND 8 offers several new logging options. You can specify what types of messages are logged, where each message type is sent, and what severity of each message type to log. In general, the default logging settings are suitable, but if you want to change them, it is recommended that you refer to other sources of BIND 8 documentation for information about logging.

Logging channels

The DNS server can log messages to different output channels. Channels specify where logging data is sent. You can select the following channel types:

- **File channels**

Messages logged to file channels are sent to a file. The default file channels are as400_debug and as400_QPRINT. By default, debug messages are logged to the as400_debug channel, which is the NAMED.RUN file, but you can specify to send other message categories to this file as well. Message categories logged to as400_QPRINT are sent to a QPRINT spool file for user profile QTCP. You can create your own file channels in addition to the default channels provided.

- **Syslog channels**

Messages logged to this channel are sent to the servers job log. The default syslog channel is as400_joblog. Logging messages routed to this channel are sent to the joblog of the DNS server instance.

- **Null channels**

All messages logged to the null channel will be discarded. The default null channel is as400_null. You can route categories to the null channel if you do not want the messages to appear in any log file.

Message categories

Messages are grouped into categories. You can specify what message categories should be logged to each channel. There are many categories, including:

- config: Configuration file processing
- db: Database operations
- queries: Generates a short log message for every query the server receives
- lame-servers: Detection of bad delegations
- update: Dynamic updates
- xfer-in: Zone transfers the server is receiving
- xfer-out: Zone transfers the server is sending

Log files can become 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.

Message severity

Channels allow you to filter by message severity. For each channel, you can specify the severity level for which messages are logged. The following severity levels are available:

- Critical
- Error
- Warning
- Notice
- Info
- Debug (specify debug level 0-11)
- Dynamic (inherit the server startup debug level)

All messages of the severity you select and any levels above it in the list are logged. For example, if you select Warning, the channel logs Warning, Error, and Critical messages. If you select Debug level, you can specify a value from 0 to 11 for which you want debug messages to be logged.

Changing logging settings

To access logging options, follow these steps:

1. In iSeries Navigator, expand *your system* → **Network** → **Servers** → **DNS**.
2. In the right pane, right-click *your DNS server* and select **Configuration**.
3. In the DNS configuration window, right-click **DNS server** and select **Properties**.
4. In the Server Properties window, select the **Channels** tab to create new file channels or properties of a channel, such as the severity of messages logged to each channel.
5. In the Server Properties window, select the **Logging** tab to specify which message categories are logged to each channel.

Troubleshoot tip

The as400_joblog channel default severity level is set to Error. This setting is used to reduce the volume of informational and warning messages, which can otherwise degrade performance. If you are experiencing problems but the joblog is not indicating the source of the problem, you might need to change the severity level. Follow the procedure above to access the Channels page and change the severity level for the as400_joblog channel to Warning, Notice, or Info so you can view more logging data. After you have resolved the problem, reset the severity level to Error to reduce the number of messages in the joblog.

Changing Domain Name System debug settings

The Domain Name System (DNS) debug function can provide information that can help you determine and correct DNS server problems.

DNS offers 12 levels of debug control. Logging typically provides an easier method of finding problems, but in some cases debugging might be necessary. Under normal conditions, debugging is turned off (value = 0). It is recommended that you first use logging to attempt to correct problems.

Valid debug levels are 0 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 the NAMED.RUN file in your i5/OS directory path: Integrated File System/Root/QIBM/UserData/OS400/DNS/<server instance>, where <server instance> is the name of the DNS server instance. The NAMED.RUN file continues to grow as long as the debug level is set to 1 or higher, and the DNS server continues to run. You can also use the **Server Properties - Channels** page to specify preferences for maximum size and number of versions of the NAMED.RUN file.

To change the debug value for a DNS server instance, follow these steps:

1. In iSeries Navigator, expand *your system* → **Network** → **Servers** → **DNS**.
2. In the right pane, right-click *your DNS server* and select **Configuration**.
3. In the DNS configuration window, right-click the DNS server and select **Properties**.
4. On the Server Properties - General page, specify the server startup debug level.
5. If the server is running, stop and restart the server.

Note: Changes to the debug level do not take effect while the server is running. The debug level set here will be used the next time the server is fully restarted. If you need to change the debug level while the server is running, see Advanced DNS features.

Related concepts

“Advanced Domain Name System features” on page 32

DNS in iSeries Navigator provides an interface with advanced features for configuring and managing your DNS server.

Related information for Domain Name System



Listed here are the IBM Redbooks™ (in PDF format) and Web sites that relate to the Domain Name System (DNS) topic. You can view or print any of the PDFs.




IBM Redbooks

AS/400® TCP/IP Autoconfiguration: DNS and DHCP Support  (5181 KB)

This Redbook describes the Domain Name System (DNS) server and Dynamic Host Configuration Protocol (DHCP) server support that are included in i5/OS. The information in this Redbook helps you install, tailor, configure, and troubleshoot DNS and DHCP support through examples.

Web sites

- *DNS and BIND*, third edition. Paul Albitz and Cricket Liu. Published by O'Reilly and Associates, Inc.  Sebastopol, California, 1998. ISBN number: 1-56592-512-2. This is the most definitive source on DNS.
- The Internet Software Consortium Web site  contains news, links, and other resources for BIND.


- The InterNIC  site maintains a directory of all domain name registrars that are authorized by the Internet Corporation for Assigned Names and Numbers (ICANN).
- The DNS Resources Directory  provides DNS reference material and links to many other DNS resources, including discussion groups. It also provides a listing of DNS related RFCs .

Saving PDF files

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

1. Right-click the PDF in your browser (right-click the link above).
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

- 1 You need Adobe Reader installed on your system to view or print these PDFs. You can download a free
- 1 copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

- | The licensed program described in this information and all licensed material available for it are provided
- | by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement,
- | IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming Interface Information

This DNS publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

- | AFS
- | AS/400
- | iSeries
- | i5/OS
- | IBM
- | IBM (logo)
- | OS/400
- | Redbooks
- | System i

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Printed in USA