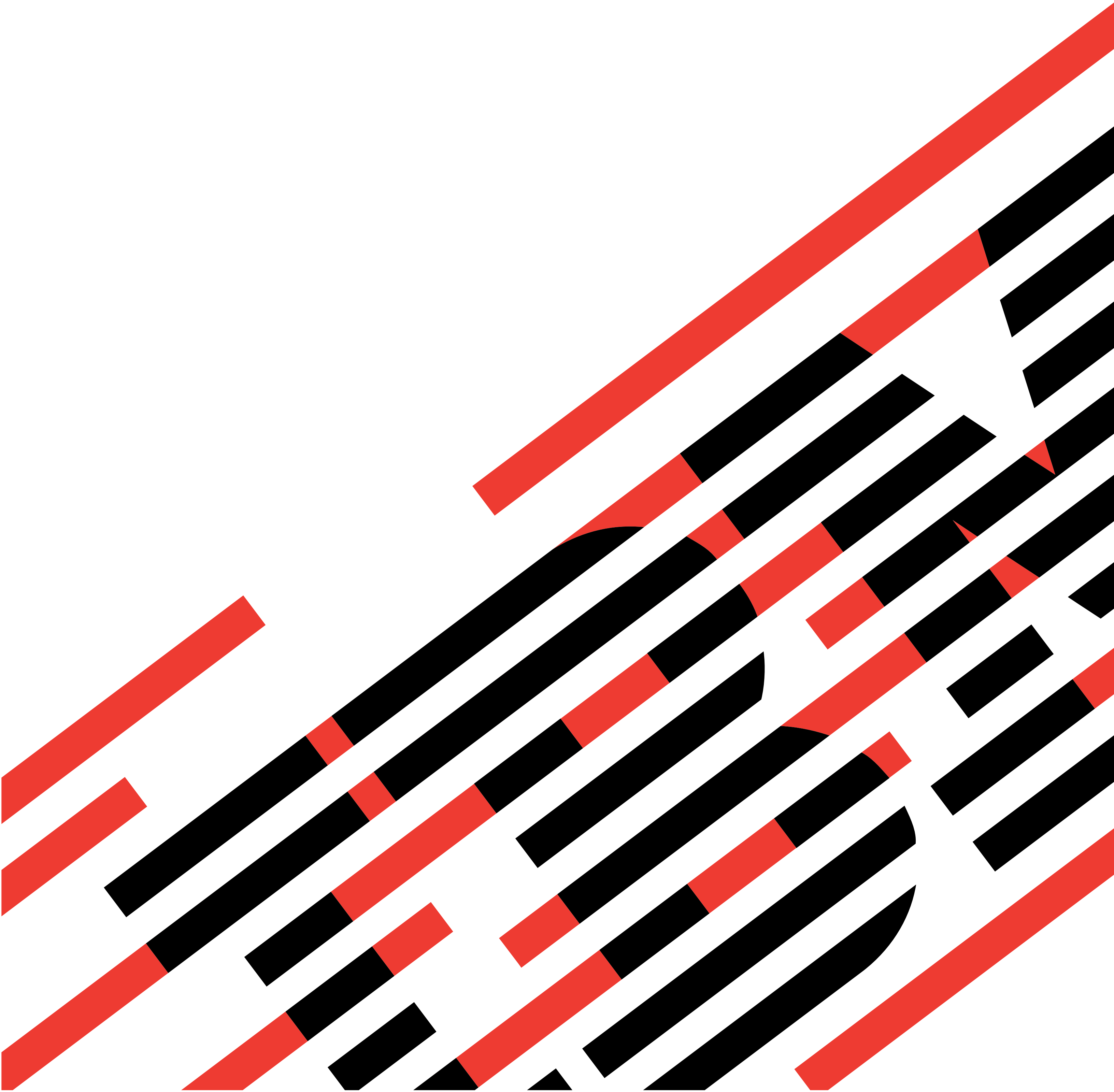
iSeries

DNS

Version 5 Release 3



IBM

eserver

iSeries

DNS

Version 5 Release 3

Note

Before using this information and the product it supports, be sure to read the information in "Notices," on page 35.

Fifth Edition (August 2005)

This edition applies to version 5, release 3, modification 0 of IBM Operating System/400 (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.

Contents

DNS

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 may 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 Version 5 Release 1 (V5R1), DNS services are based on the industry standard DNS implementation known as BIND (Berkeley Internet Name Domain) version 8. Previous OS/400(R) DNS services were based on BIND version 4.9.3. OS/400 option 33, Portable Application Solutions Environment (PASE), must be installed on your iSeries(TM) server in order to use the new BIND 8-based DNS server. If you do not have PASE installed, you can still run the same DNS server based on BIND 4.9.3 that was available in previous releases. However, migration to BIND 8 will provide improved function and incorporate 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, refer to the V4R5 DNS Information Center topic (about 357 KB) for information regarding DNS based on BIND 4.9.3.

- “Print this topic” on page 2 allows you to download or print the DNS topic.

Understanding DNS
These topics are designed to help you understand DNS fundamentals of DNS for the iSeries.

“DNS examples” on page 2 provides diagrams and explanations of how DNS works.

“DNS concepts” on page 10 explains the objects and processes that DNS uses to function.

“Planning DNS” on page 19 helps you to create a plan for your DNS configuration.

Using DNS
These topics are designed to assist you as you configure and manage DNS on your iSeries. They also explain how to take advantage of new features now available.

“DNS system requirements” on page 21
This topic describes the software requirements to run DNS on your iSeries server.

“Configuring DNS” on page 22
This topic explains how to use iSeries Navigator to configure name servers and to resolve queries outside of your domain.

“Managing DNS” on page 26
This topic discusses how to verify DNS function, monitor performance, and maintain DNS data and files.

“Troubleshooting DNS” on page 31
This topic explains DNS logging and debugging settings that can help you resolve problems with your DNS server.

If you have questions that aren’t answered in the Information Center, “Other information about DNS” on page 33 provides a list of other resources and reference materials.

Print this topic

To view or download the PDF version, select DNS (about 357 KB).

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

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

If you need Adobe Acrobat Reader to view or print these PDFs, you can download a copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

DNS examples

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 would be used. They also link to related concepts you may find useful to understanding the pictures.

“Example: Single DNS server for intranet”
Depicts a simple subnet with a DNS server for internal use.

“Example: Single DNS server with Internet access” on page 4
Depicts a simple subnet with a DNS server connected directly to the Internet.

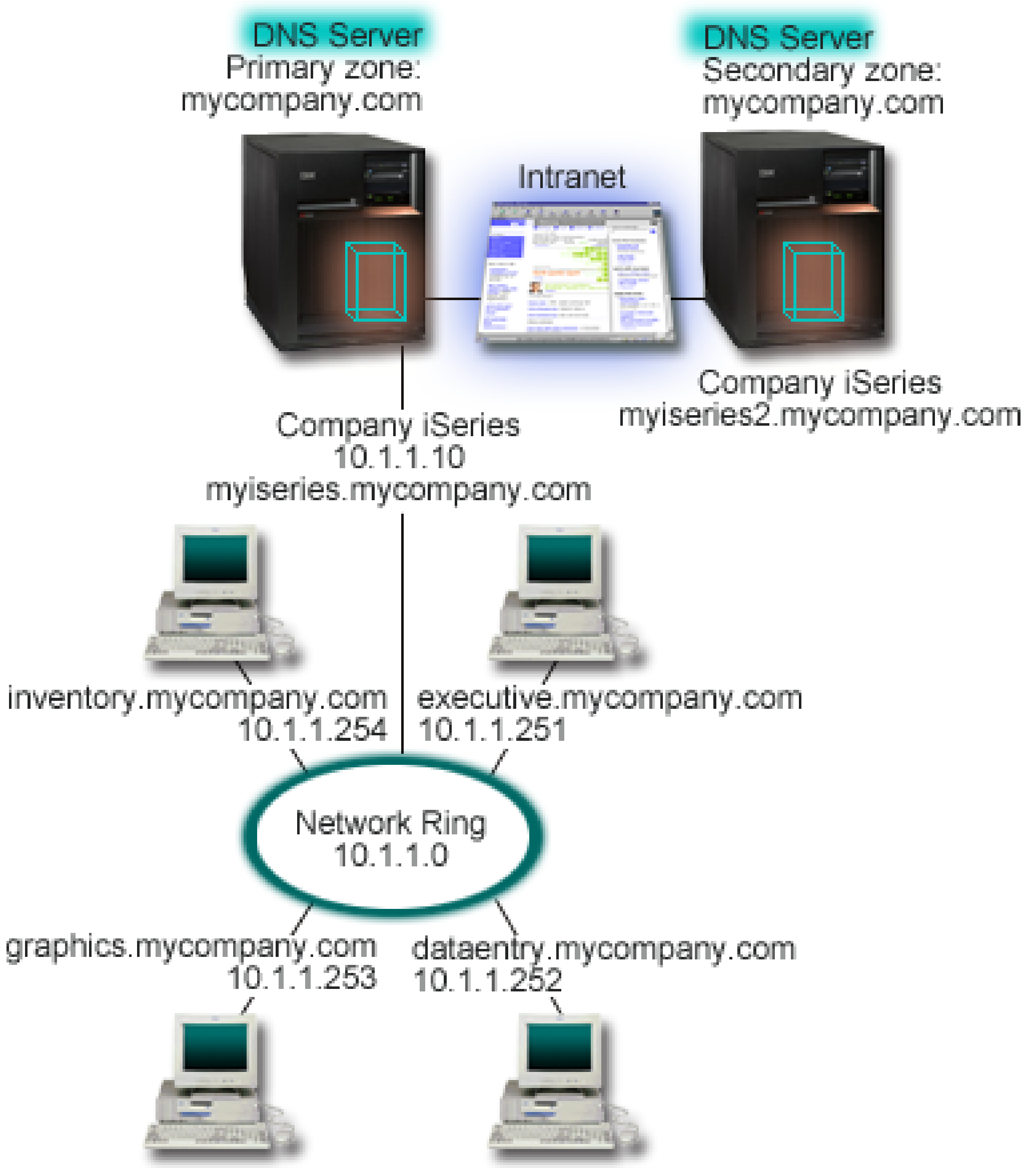
“Example: DNS and DHCP on the same iSeries$^{(TM)}$ server” on page 6
Depicts DNS and DHCP on the same server. The configuration can be used to update DNS zone data dynamically when DHCP assigns IP addresses to hosts. If your DHCP server will reside on a different iSeries, refer to Example: DNS and DHCP on different iSeries servers for additional DHCP configuration requirements.

“Example: Split DNS over firewall” on page 8
Depicts DNS operating over a firewall to protect internal data from the Internet, while allowing internal users to access data on the Internet.

Example: Single DNS server for intranet

The following illustration depicts DNS running on an iSeries$^{(TM)}$ for an internal network. This single DNS server instance is set up to listen for queries on all interface IP addresses. The server is a primary name server for the ″mycompany.com″ zone.

Figure 1. 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 “DNS resource records” on page 16. 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 may be required, depending on what other TCP/IP based applications you are running on your intranet. For example, if you are running internal e-mail systems, you may 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 could 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 myiseries server is part of an intranet. Another iSeries server, myiseries2, 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.

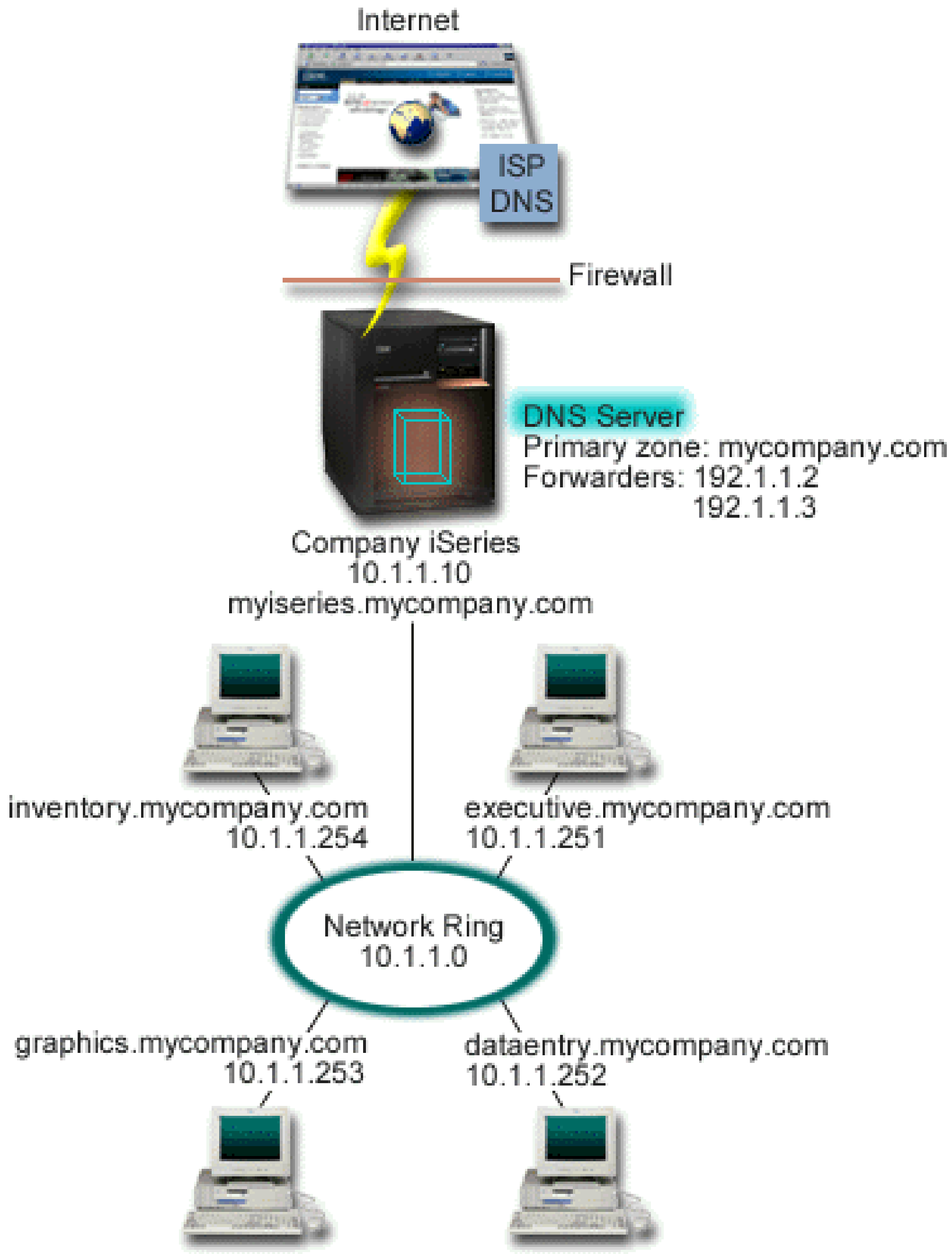
Refer to the following topics for more information about the objects discussed in this example:

- “Understanding DNS” on page 11 explains what DNS is and how it works. It also defines the different types of zones that can be defined on a DNS server.
- “DNS resource records” on page 16 explains how resource records are used by DNS.

Example: Single DNS server with Internet access

The following illustration depicts the same example network from the “Example: Single DNS server for intranet” on page 2 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 1. Single DNS server with Internet access.



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

Define Internet root servers
You can load the default Internet root servers automatically, but you may need to update the list. These servers will help to resolve addresses outside of your own zone. For instructions for obtaining the current Internet root servers, refer to “Accessing external DNS data” on page 26.

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 will need to set the **forward** option to **first**. The server will first try forwarding and then query the root servers only if forwarding fails to resolve the query.

The following configuration changes may 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 will be determined by your ISP and other networking factors.

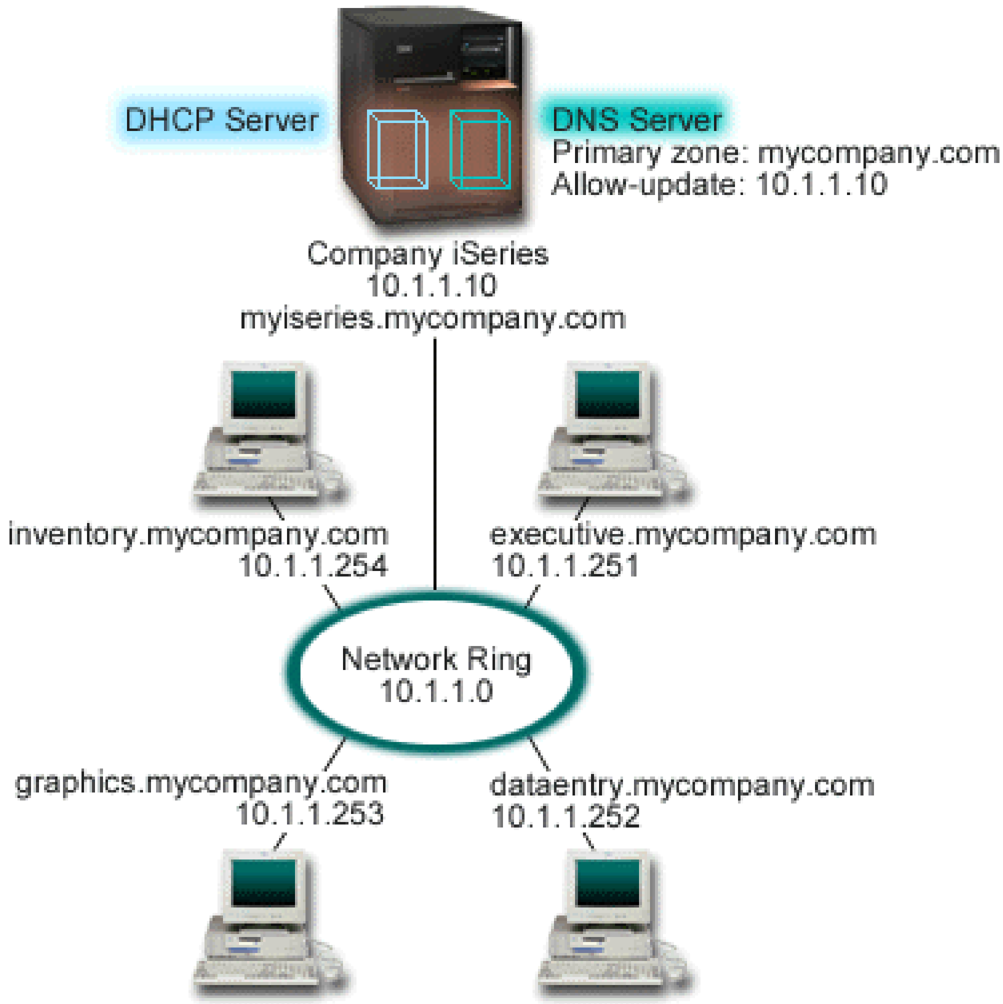
Register your domain name
If you will be visible to the Internet, and if you haven't already registered, you will need to "Setting up your DNS domain" on page 14.

Establish a firewall
It is not recommended that you allow your DNS to be directly connected to the Internet. You should configure a firewall or take other precautions to secure your iSeries(TM). For more information, refer to IBM(R) Secureway: iSeries and the Internet in the Information Center.

Example: DNS and DHCP on the same iSeries(TM) server

The following figure depicts a small subnet network with one iSeries server acting 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 1. DNS and DHCP on the same iSeries server.



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 changed because it is assigned by DHCP, then its dependent clients would be unable to map a network drive to its host name because the DNS records would contains the file server's previous IP address.

With the V5R1 DNS server based on BIND 8, you can configure your DNS zone to accept "Dynamic updates" on page 14 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 would be updated dynamically. This would allow 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 would 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 may want to configure a separate dynamic zone to minimize the need for manual updates. Refer to "Determining domain structure" on page 20 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 would have allow-update data, but other zones defined on the server could 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. For more information on configuring the DHCP server to send dynamic updates, refer to Configuring DHCP to send dynamic updates.

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 will enable IXFR-enabled secondary servers to track and load only the updated zone data, instead of the entire zone.

If you will be running DNS and DHCP on different servers, there are some additional configuration requirements for the DHCP server. For more information, refer to Example: DNS and DHCP on different iSeries servers.

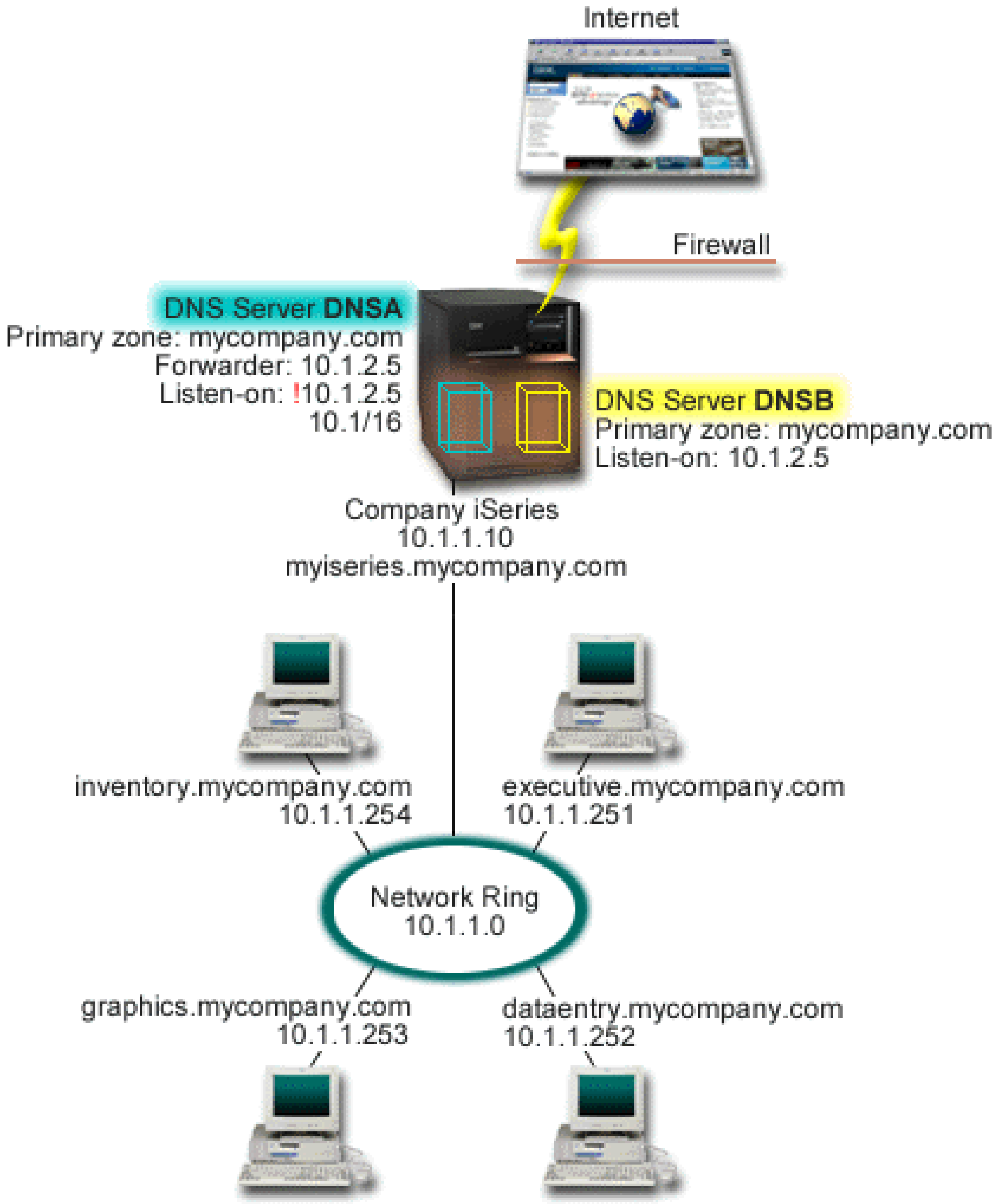
Example: Split DNS over firewall

The following illustration depicts a simple subnet network that uses a firewall for security. V5R1 DNS based on BIND 8 allows you to set up multiple DNS servers on a single iSeries(TM). Suppose 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 iSeries, one for the intranet and one for everything in its public domain. This is called split DNS.

Figure 1. 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 will force 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 will need to be configured to query only the DNSA server. You will need to consider the following configuration settings to set up split DNS:

Listen-on
In previous examples, there has been only one DNS server on an iSeries. It was set to listen on all interface IP addresses. Whenever you have multiple DNS servers on an iSeries, you have to 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 coming in from the firewall will be 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 will be 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 would be compared to the first element and would immediately be denied.

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

DNS concepts

V5R1 DNS offers new features based on BIND 8. The following links provide overviews of how DNS works and new features you can use:

Basic DNS function:

“Understanding DNS” on page 11
Provides an overview of what DNS is and how it works, as well as a description of the types of zones you can define.

“Understanding DNS queries” on page 12
Explains how DNS resolves queries on behalf of clients.

“Setting up your DNS domain” on page 14
Provides an overview of domain registration, with links to other reference sites for setting up your own domain space.

New DNS features:

“Dynamic updates” on page 14
V5R1 DNS based on BIND 8 supports dynamic updates. These allow outside sources, such as DHCP, to send updates to the DNS server.

“BIND 8 features” on page 15
Besides dynamic updates, BIND 8 offers several new features to enhance performance of your DNS server.

Resource record reference:

“DNS resource records” on page 16
Resource records are used to store data about domain names and IP addresses. This topic contains a searchable list of resource records supported for V5R1.

“Mail and MX records” on page 19
DNS supports advanced mail routing through the use of these records.

There are many outside sources that explain DNS in greater detail. Refer to “Other information about DNS” on page 33 for additional reference sources.

Understanding DNS

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 may 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 considered 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” on page 12 explains the paths a client can use to resolve a query.

Understanding zones

DNS data is divided into manageable sets of data called zones. 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 may make 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 iSeries(TM) DNS to define several types of zones to help you manage DNS data:

Primary zone
Loads zone data directly from a file on a host. A primary zone may contain a subzone, or child zone. It may 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 “DNS resource records” on page 16 may be associated with a host.

Secondary zone
Loads zone data from a zone’s primary server or another secondary server. A secondary server maintains a complete copy of the zone for which it is a secondary.
Note: Secondary zones are sometimes referred to as ″slave zones″ in other BIND documentation.

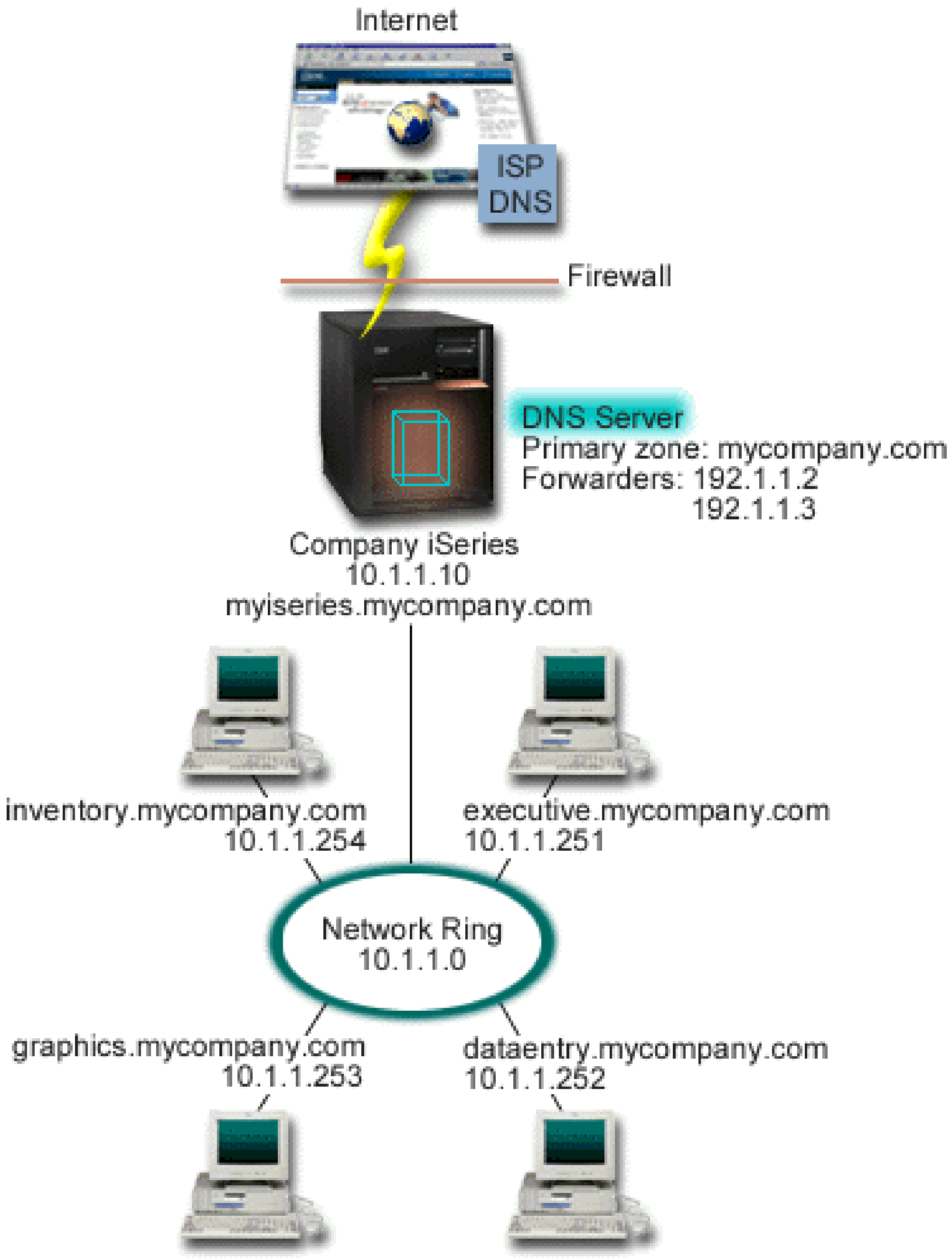
Stub zone
A stub zone is similar to a secondary zone, but it only transfers the name server (NS) records for that zone.

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

Understanding DNS queries

Clients use DNS servers to find information for them. The request may 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 usually the Internet (IN) class. The following figure depicts the sample network from the “Example: Single DNS server with Internet access” on page 4 example.

Figure 1. Single DNS server with Internet access.



Suppose host *dataentry* queries the DNS server for ″graphics.mycompany.com″. The DNS server will use its own zone data and respond 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 it receives that query. A client can attempt to contact other DNS servers on its own behalf to resolve a name. In this process, called iteration, the client uses separate and additional queries based on referral answers from servers.

Setting up your DNS domain

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

Domain registration may 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).

There are many other sources that provide information about registering and preparing to host a DNS domain. Refer to “Other information about DNS” on page 33 for additional assistance.

Dynamic updates

Dynamic Host Configuration Protocol (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 “DNS resource records” on page 16 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 will be 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 each 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 iSeries(TM) server, between different iSeries servers, or between an iSeries and other servers that are capable of dynamic updates. Refer to the following topics for more information about configuring dynamic updates for your iSeries:

- “Configuring DNS to receive dynamic updates” on page 24
- Configuring DHCP to send dynamic updates
- The dynamic update API QTOBUPT is required on servers that are sending dynamic updates to DNS. It is installed automatically with OS/400(R) Option 31, DNS.

BIND 8 features

DNS has been redesigned to use BIND 8 for V5R1. If you do not have PASE installed, you can continue to configure and run the previously released OS/400(R) DNS server based on BIND 4.9.3. “DNS system requirements” on page 21 explains what you need to run BIND 8-based DNS on your iSeries(TM). Using the new DNS allows you to take advantage of the following features:

Multiple DNS servers running on a single iSeries

In past releases, only one DNS server could 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. Refer to the example “Example: Split DNS over firewall” on page 8 for more information about split DNS.

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 could set forwarding at a global level, but add exceptions to domains for which you want to force normal iterative resolution. Or, you could set normal iterative resolution at the global level, then force forwarding within certain domains.

Secure dynamic updates

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

For more information about dynamic updates, refer to “Dynamic updates” on page 14. For more information about authorizing updates from external sources, refer to “Planning security measures” on page 21.

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 to all known secondary servers that indicates data has changed. Secondary servers may 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, and 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.

DNS resource records

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.

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 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.
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.

Resource record	Abbreviation	Description
Location records	LOC	The LOC record specifies the physical location of network components. These records could 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 SMTP (Simple Mail Transfer Protocol) to locate hosts that will process or forward 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 will be 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.
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 could be for a zone, a user, or a host. This record type is defined in RFC 2065.

Resource record	Abbreviation	Description
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.
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 may 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 iSeries DHCP for dynamic updates. The DHCP server writes an associated TXT record for each PTR and A record update done by the DHCP server. DHCP records will 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.

Resource record	Abbreviation	Description
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.

Mail and MX records

Mail and MX records are used by mail routing programs such as Simple Mail Transfer Protocol (SMTP). Refer to the lookup table in "DNS resource records" on page 16 for more information about the types of mail records supported by iSeries$^{(TM)}$ DNS.

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

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

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

A DNS server can respond with an empty list of MX resource records when the name is in the DNS server's authority but has no MX assigned to it. When this occurs, the sending mail application may try to establish a connection with the destination host directly. **Note:** Using a wild card (example: `*.mycompany.com`) in MX records for a domain is not recommended.

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

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

Planning DNS

DNS offers a variety of solutions. Before you configure DNS, it is important to plan how it will work within your network. Subjects such as network structure, performance, and security should be assessed before you implement DNS. Consider the topics below to plan for your DNS needs:

“Determining DNS authorities”
There are special authorization requirements for the DNS administrator. You should also consider security implications of authorization. This topic explains the requirements.

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

“Planning security measures” on page 21
DNS provides security options to limit outside access to your server. This topic explains the options and how to control access.

Determining DNS authorities

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 iSeries(TM) administrator to configure and administer DNS. Granting all object access ensures that the administrator is capable of performing DNS administrative tasks. It is recommended that users who will be configuring 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 “Maintaining DNS configuration files” on page 28 must be granted.

Determining domain structure

It is important to determine how you will 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 “Other information about DNS” on page 33 book for in-depth guidelines.

If you configure a DNS zone as a dynamic zone, you cannot make manual changes to zone data while the server is running. Doing so could cause interference with incoming dynamic updates. If it is necessary to make manual updates, stop the server, make the changes, then restart the server. Dynamic updates sent to a stopped DNS server will never be completed. For this reason, you may want to configure a dynamic zone and a static zone separately. You could 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.

iSeries(TM) DNS provides a graphical interface for configuring your servers. In some cases, the interface uses terminology or concepts that may be represented differently in other sources. If you refer to other information sources when you are planning for your DNS configuration, it may be helpful to remember the following:

- All zones and objects defined in a server 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.
- iSeries DNS refers to **primary zones** and **secondary zones**. These are sometimes referred to as master zones and slave zones in other BIND documentation.
- 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

Securing your DNS server is essential. In addition to the security considerations below, DNS security and iSeries$^{(TM)}$ security are covered in a variety of sources including IBM$^{(R)}$ Secureway: iSeries and the Internet in the Information Center. The book “Other information about DNS” on page 33 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 simply 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 will be 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 would be compared to the first element and would immediately be denied.

If the elements were reversed (10.1.1/24; !10.1.1.5), the IP address 10.1.1.5 would be allowed access because the server would 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 Access Control Lists 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 will not accept queries from or use to resolve a query. Queries from these addresses will not be responded to.

DNS system requirements

The DNS option (Option 31) does not install automatically with the base operating system. You must specifically select DNS for installation. The new DNS server added for V5R1 is based on the industry standard DNS implementation known as BIND 8. Previous OS/400$^{(R)}$ DNS services were based on BIND 4.9.3, and are still available in V5R1.

Once DNS is installed, you will by default be 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 Portable Application Solutions Environment (PASE). PASE is SS1 Option 33. Once PASE is installed, iSeries Navigator will automatically handle 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. Refer to the V4R5 DNS Information Center topic (about 357 KB) for BIND 4.9.3 documentation.

If you want to configure a DHCP server on a different iSeries to send updates to this DNS server, Option 31 must be installed on DHCP iSeries as well. The DHCP server uses programming interfaces provided by Option 31 to perform dynamic updates.

To determine whether DNS is installed, follow these steps:

1. At the command line, type **GO LICPGM** and press **Enter**.
2. Type **10** (Display installed licensed programs) and press **Enter**.
3. Page down to **5722SS1 OS/400 - 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          OS/400 - Domain Name System
   ```
4. Press **F3** to exit the display.

To install DNS, follow these steps:

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

Configuring DNS

Before you work with your DNS configuration, refer to “DNS system requirements” on page 21 to install the necessary DNS components. The following subtopics provide guidelines for configuring your DNS server:

“Accessing DNS in iSeries Navigator” on page 23
Instructions for accessing DNS in iSeries Navigator.

“Configuring name servers” on page 23
DNS allows you to create multiple name server instances. This topic provides instructions for configuring a name server.

“Configuring DNS to receive dynamic updates” on page 24
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 DNS files” on page 25
DNS can import existing zone data files. Follow these time-saving procedures for creating a new zone from an existing configuration file.

“Accessing external DNS data” on page 26
When you create DNS zone data, your server will be able to resolve queries to that zone. This topic explains how to configure DNS to resolve queries outside of your domain.

Accessing DNS in iSeries Navigator

The following instructions will 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. Refer to the V4R5 DNS Information Center topic (about 62 pages) 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 iSeries server** —> **Network** —> **Servers** —> **DNS**.
2. Right-click **DNS** and select **New Configuration**.

If you have a pre-V5R1 DNS server configured, follow these steps:

1. In **iSeries Navigator**, expand **your iSeries server** —> **Network** —> **Servers** —> **DNS**.
2. In the right pane, double-click the DNS server to open the **DNS Configuration** window.
3. If you are using PASE, you will be offered the option to migrate your existing DNS configuration to the BIND 8 implementation. However, once you migrate to BIND 8, you cannot revert to BIND 4.9.3. If you are unsure, select **No**. If you want to migrate, select **Yes**.
4. To migrate your DNS server to BIND 8 at any time, right-click **DNS** from the left pane and select **Migrate to Version 8**.

Configuring name servers

iSeries(TM) DNS based on BIND 8 supports multiple name server instances. The tasks below guide you through the process of creating a single name server instance, including its properties and zones.

1. “Creating a name server instance”
   Use the **New DNS Configuration** wizard to define a DNS server instance.
2. “Editing DNS server properties” on page 24
   Define the global properties for your new server instance.
3. “Configuring zones on a name server” on page 24
   Create zones and zone data to populate your name server.

If want to create multiple instances, repeat the procedure above 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. For more information about configuration files, refer to “Maintaining DNS configuration files” on page 28.

Creating a name server instance

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

1. In **iSeries Navigator**, expand **your iSeries(TM) server** —> **Network** —> **Servers** —> **DNS**.
2. In the left pane, right-click **DNS** and select **New Name Server...**
3. The wizard will guide you through the configuration process.

The wizard will require 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 may 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.

What to do next: "Editing DNS server properties."

Editing DNS server properties

After you create a name server, you can edit properties such as allow-update and debug levels. These options will apply only to the server instance you are changing. To edit the properties of the DNS server instance, follow these steps:

1. In **iSeries Navigator**, expand **your iSeries$^{(TM)}$ server** —> **Network** —> **Servers** —> **DNS**.
2. In the right pane, right-click **your DNS server** and select **Configuration**.
3. Right-click **DNS Server** and select **Properties**.

What to do next: "Configuring zones on a name server."

Configuring zones on a name server

Once you have created your name server, return to the **iSeries Navigator** main window. Your server will be displayed in the right pane. To configure zones on your server, right-click the server name and select **Configuration**. The **DNS Configuration** window displays.

All zones are configured using wizards. Create **Forward Lookup Zones** or **Reverse Lookup Zones** by right-clicking the corresponding folder. The options for that zone type will display. Select the zone type you want to create to start the wizard.

For descriptions of the types of objects you can create in V5R1 DNS, refer to "Understanding DNS" on page 11.

Once you have configured your zones, you may want to refer to these topics for more configuration information:

"Configuring DNS to receive dynamic updates"
Dynamic updates allow authorized sources to send resource records to update zone data. This can reduce the need for manual zone data changes.

"Importing DNS files" on page 25
If you have an existing zone data file from another DNS server, you can upload it to your new server.

"Accessing external DNS data" on page 26
You may want to configure your server to resolve queries for information ouside of the zone data it contains. You can forward queries to other authoritative servers or load root servers to help resolve queries.

Configuring DNS to receive dynamic updates

When creating dynamic zones, you should consider your network structure. If parts of your domain will still require manual updates, you may want to consider setting up separate static and dynamic zones. If you have 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 did not stop the server, you would lose all dynamic updates that were processed since it was started. However, stopping the server to make manual updates means you could 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 iSeries server** —> **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 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.

If you are setting up DNS to receive dynamic updates from an iSeries DHCP server, refer to Configuring DHCP to send dynamic updates.

Importing DNS files

You can create a primary zone by importing a zone data file, or by converting existing host tables. Refer to *Converting host tables* in the V4R5 DNS Information Center topic (about 357 KB) 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 will verify that it is a valid zone data file and add it to the NAMED.CONF file for this server instance.

To import a zone file, follow these steps:

1. In **iSeries Navigator**, expand **your iSeries(TM) server** —> **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.

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.

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

Accessing external DNS data

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 a DNS server looks is the root servers. The root servers direct a DNS server towards other servers in the hierarchy until an answer is found, or it is determined that there is no answer.

iSeries^(TM) 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.

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

1. Anonymous FTP to the InterNIC server: `FTP.RS.INTERNIC.NET`
2. Download this file: `/domain/named.root`
3. Store the file in the following directory path: `Integrated File System/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE`.

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

Intranet root servers
If your DNS server is part of a large intranet, you may 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.

Managing DNS

Once you have DNS configured, you may want to review the following topics:

"Verifying DNS function with NSLookup" on page 27
You can use NSLookup to verify that DNS is working.

"Security key management" on page 27
Security keys allow you to limit access to your DNS data.

"DNS server statistics" on page 28
Database dump and statistics tools can help you review and manage server performance.

"Maintaining DNS configuration files" on page 28
Understand the files DNS uses, and review guidelines for backing up and maintaining them.

"Advanced DNS features" on page 30
This topic discusses how experienced administrators can access advanced features.

Verifying DNS function with NSLookup

Use NSLookup (Name Server Lookup) to query the DNS server for an IP address. This verifies that the DNS server is responding to queries. Request the host name that is associated with the loopback IP address (127.0.0.1). It should respond with the host name (localhost). You should also query specific names that are defined in the server instance 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**.

Security key management

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.

DNS keys

The DNS key is a key defined for BIND. It is 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 iSeries$^{(TM)}$ server** —> **Network** —> **Servers** —> **DNS**.
2. In the right pane, right-click the DNS server instance you want to open and select **Configuration**.
3. In the **DNS Configuration** window, select **File** > **Manage Keys...**

Dynamic update keys

Dynamic update keys are used for securing dynamic updates by the DHCP server. These keys must be present when DNS and DHCP are on the same iSeries. If DHCP is on a different iSeries, you must create the same dynamic update key on each iSeries server to allow secure dynamic updates.

To manage dynamic update keys, follow these steps:

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

DNS server statistics

DNS provides several diagnostic tools. They can be used to monitor performance of your server.

Server Statistics
DNS allows you to view the statistics for a server instance. These statistics summarize the number of queries and responses the server received since the last time the server restarted or reloaded its database. Information is continually appended to this file until you delete the file. This information may 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 iSeries(TM) server** —> **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**.

Active server database
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. The 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. This information may be useful in tracking down problems.

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 iSeries 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 iSeries server** —> **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 DNS configuration files

You can use OS/400(R) DNS to create and manage DNS server instances on your iSeries(TM). The configuration files for DNS are managed by iSeries Navigator. You should 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, refer to *Backing up DNS configuration files and maintaining log files* in the V4R5 DNS Information Center topic 📖 (about 62 pages).

In the table below, files are listed in the heirarchy 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		**Description**
QIBM/UserData/OS400/DNS/		Starting point directory for DNS.
ATTRIBUTES	💾	DNS uses this file to determine which BIND version you are using.

Name		Description
QIBM/UserData/OS400/DNS/*<instance-n>*/		Starting point directory for a DNS instance.
ATTRIBUTES	💾	Configuration attributes used by iSeries 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 "DNS server statistics" on page 28.
NAMED.STATS	✖	"DNS server statistics" on page 28.
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.
.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).

Name		**Description**
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.

Advanced DNS features

DNS in iSeries Navigator provides an interface for configuring and managing your DNS server. The following tasks are provided as shortcuts for administrators who are familiar with the iSeries graphical interface. They provide fast methods for changing server status and attributes for multiple instances at once.

Changing DNS attributes

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 will 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 DNS servers
The 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 `ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL)` at the command line.

Changing debug values
DNS in the iSeries Navigator interface does not allow you to change the debug level while the server is running. However, you can use character-based interface to change the debug level while the server is running. This feature can be useful to administrators who have large zones and they do not want the large amount of debug data that they would get while the server is first starting up and loading all of the zone data. 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 `ADDLIBLE 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 DNS

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 may 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.

“DNS server logging” on page 32
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.

“DNS debug settings” on page 33
DNS offers 12 levels of debug control. Logging will usually provide an easier method of finding problems, but in some cases debugging may be necessary. Under normal conditions, debugging is turned off (value = 0).

“Other information about DNS” on page 33
General DNS troubleshooting information is available from many sources. In particular, the O’Reilly DNS and BIND book is a good reference for general questions, and the DNS resources directory provides links to discussion groups for DNS administrators.

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* in the V4R5 DNS Information Center topic (about 357 KB).

- 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 would be QTOBDINST1 and QTOBDINST2.

DNS server logging

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 will be suitable, but if you want to change them, it is recommended that you refer to other "Other information about DNS" on page 33 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 iSeries$^{(TM)}$ server** —> **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.

Troubleshooting 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 could otherwise degrade performance. If you are experiencing problems but the joblog is not indicating the source of the problem, you may 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. Once you have resolved the problem, reset the severity level to Error to reduce the number of messages in the joblog.

DNS debug settings

The DNS debug function can provide information that may help you determine and correct DNS server problems. 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 iSeries 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. It is recommended that you delete the file from time to time to keep it from taking up too much disk space. 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 iSeries server** —> **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, refer to “Advanced DNS features” on page 30

Other information about DNS

There are many sources of information regarding DNS and BIND 8. The following list is only a small representation of the resources available:

- 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 .

IBM Manuals and Redbooks(TM)

- AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support

  This redbook describes the Domain Name System (DNS) server and Dynamic Host Configuration Protocol (DHCP) server support that are included in OS/400(R). The information in this redbook helps you install, tailor, configure, and troubleshoot DNS and DHCP support through examples.
  Note: This redbook has not been updated to include the new BIND 8 features available for V5R1. However, it is a good reference for general DNS concepts.

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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
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, 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 49XA
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, or any equivalent agreement between us.

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

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:
Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance, and WordPro are trademarks of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.

ActionMedia, LANDesk, MMX, Pentium, and ProShare are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Terms and conditions for downloading and printing publications

Permissions for the use of the publications you have selected for download are granted subject to the following terms and conditions and your indication of acceptance thereof.

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 AND FITNESS FOR A PARTICULAR PURPOSE.

All material copyrighted by IBM Corporation.

By downloading or printing a publication from this site, you have indicated your agreement with these terms and conditions.

Printed in USA