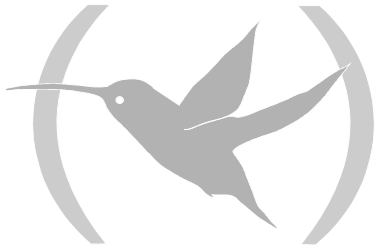
Router Teldat

Cliente DNS

Doc. *DM723* Rev. *10.00*
Marzo, 2003

ÍNDICE

Capítulo 1
Domain Name System



1. Introducción

El Sistema de Nombres de Dominio (Domain Name System), más conocido como DNS, es un protocolo estándar descrito en las RFCs 1034 y 1035. Permite a los usuarios de red utilizar nombres jerárquicos sencillos para referirse a otros equipos. De esta forma, el usuario puede obviar la dirección IP asociada al equipo y referirse a él con un nombre más fácil de memorizar. Además, facilita el cambio en la dirección IP de un equipo: los cambios de dirección sólo deben notificarse al servidor DNS encargado de ese equipo, siendo transparentes para el usuario, que sigue refiriéndose al equipo con el mismo nombre.

DNS es un protocolo de aplicación y usa tanto UDP como TCP. Los clientes solicitan a los servidores de DNS sus consultas por medio de UDP para hacer más rápida la comunicación y utilizan TCP sólo en caso de que llegara a ocurrir una respuesta truncada.

El DNS usa el concepto de *espacio de nombres distribuido*. Los nombres simbólicos se agrupan en *zonas de autoridad*, o más comúnmente, *zonas*. En cada una de estas zonas, uno o más equipos tienen la tarea de mantener una base de datos de nombres simbólicos y direcciones IP y de suministrar la función de servidor para los clientes que deseen traducir nombres simbólicos a direcciones IP. Estos *servidores de nombres* locales se interconectan lógicamente en una árbol jerárquico de *dominios*. Cada zona contiene una parte del árbol o *subárbol* y los nombres de esa zona se administran con independencia de los de otras zonas. La autoridad sobre zonas se delega en los servidores de nombres. En los puntos en los que un dominio contiene un subárbol que cae en una zona diferente, se dice que los servidores de nombres con autoridad sobre el dominio superior *delegan autoridad* a los servidores de nombres con autoridad sobre los subdominios. Los servidores de nombres también pueden delegar autoridad en sí mismos; en este caso, el espacio de nombres sigue dividido en zonas, pero la autoridad para ambas la ejerce el mismo servidor.

El resultado de este esquema es:

- En vez de tener un servidor central para la base de datos, el trabajo implicado en mantenerla se reparte entre los hosts a lo largo y ancho del espacio de nombres.

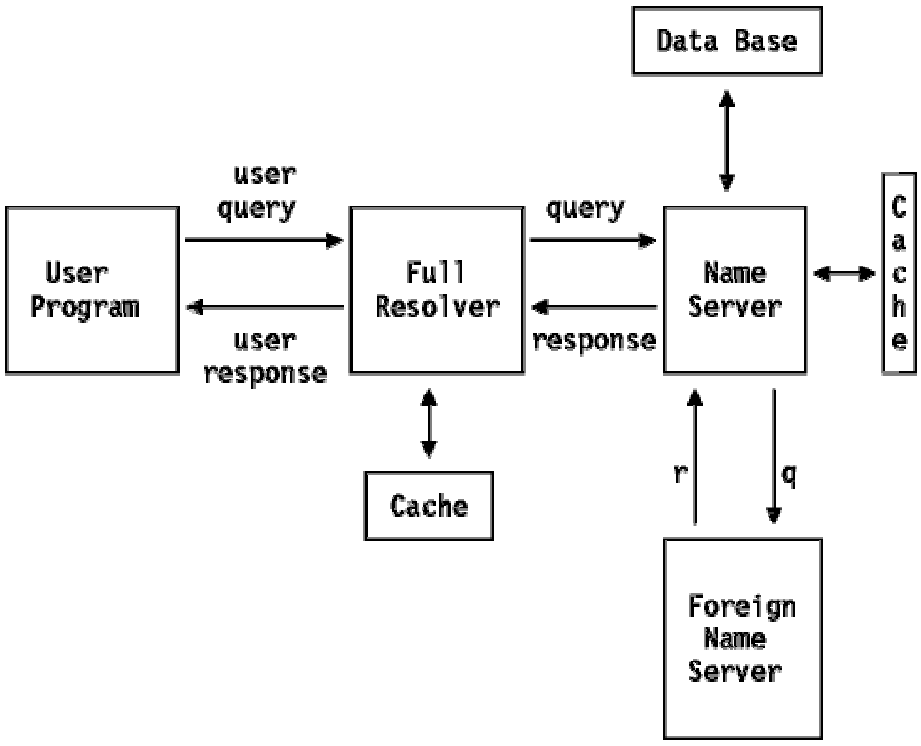
- La autoridad para crear y cambiar nombres simbólicos de hosts y la responsabilidad de mantener una base de datos para ellos le corresponde a la organización propietaria de la zona que los contiene.
- Desde el punto de vista del usuario, hay una sola base de datos que trata la resolución de las direcciones.

2. Resolución de dominios

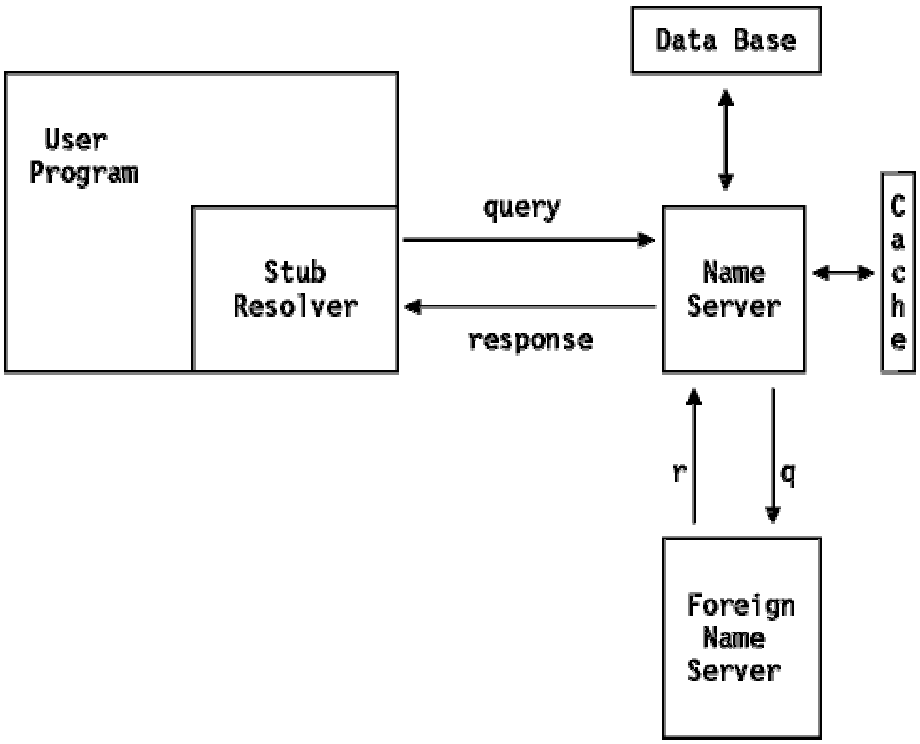
La resolución de nombres de dominio es un proceso cliente-servidor. El cliente DNS más habitual realiza peticiones a los servidores de nombres para obtener la dirección IP asociada a un nombre de dominio. Este tipo de peticiones se denominan peticiones estándar. Aparte de estas peticiones hay peticiones inversas para obtener el nombre de un dominio a partir de la dirección IP y peticiones genéricas, para obtener algún otro dato adicional de un dominio.

Se pueden distinguir dos tipos de resolvedores:

- Resolvedor completo (full resolver): resolvedor propiamente dicho, realiza las peticiones necesarias para obtener la información deseada. Analiza las respuestas recibidas del servidor para ver si ha recibido la respuesta a la petición realizada o una delegación a otro servidor. En este último caso lanza nuevas peticiones hasta conseguir la respuesta deseada.
- Resolvedor simple (stub resolver): delega la resolución de la petición en un resolvedor completo. El resolvedor tiene configuradas las direcciones IP de una serie de servidores capaces de realizar el proceso de petición completo: lanza la petición deseada y espera a que le llegue la respuesta a la petición, no admitiendo respuestas que incluyan delegaciones en otros servidores.



Esquema de funcionamiento del resolvedor completo (full resolver)



Esquema de funcionamiento del resolvedor simple (stub resolver)

2.1. Funcionamiento del resolvedor de nombres de dominio

Las peticiones sobre nombres de dominio pueden ser de dos tipos: *recursivas* o *iterativas* (llamadas también *no-recursivas*). Un bit de flag en la consulta especifica si el cliente desea una consulta recursiva y un bit de flag en la respuesta indica si el servidor soporta peticiones recursivas. La diferencia entre una consulta recursiva y una iterativa aparece cuando el servidor recibe una solicitud a la que por sí mismo no puede dar una respuesta completa. Una consulta recursiva demanda que el servidor lance a su vez una consulta para determinar la información buscada y luego devolvérsela al cliente. Una consulta iterativa implica que el servidor de nombres debería devolver la información de la que disponga además de una lista de servidores adicionales con los que el cliente puede contactar para completar su consulta.

Las respuestas de nombres de dominio pueden ser de dos tipos: *autoritativas* y *no-autoritativas*. Un bit de flag en la respuesta indica de qué tipo es la respuesta. Cuando un servidor de nombres recibe una consulta para un dominio en una zona en la que tiene autoridad, devuelve una respuesta con el bit de flag activo. Si no tiene autoridad en esa zona, su reacción depende de si el flag de recursividad está o no activo.

Si el flag de recursividad está activo y el servidor la soporta, dirigirá su consulta a otro servidor de nombres. Este será un servidor con autoridad sobre el dominio de la consulta, o uno de los servidores de nombres de la raíz. Si el segundo servidor no devuelve una respuesta autoritativa, el proceso se repite.

Cuando un servidor (o un "full resolver") recibe una respuesta, lo cacheará para mejorar el rendimiento de consultas repetidas. La entrada de la cache se almacena con un tiempo máximo

especificado en la respuesta en un campo *TTL ("time to live")* de 32 bits. 172.800 segundos (dos días) es un valor típico.

Si el flag de recursividad no está activo o el servidor no soporta consultas recursivas, devolverá la información que tenga en su caché y una lista de servidores capaces de dar respuestas autoritativas.

2.2. Funcionamiento del servidor de nombres de dominio

Cada servidor de nombres tiene *autoridad* para cero o más zonas. Hay tres tipos de servidor de nombres:

- primario: un servidor de nombres primario carga del disco la información de una zona, y tiene autoridad sobre ella.
- secundario: un servidor de nombres secundario tiene autoridad sobre una zona, pero obtiene la información de esa zona de un servidor primario utilizando un proceso llamado *transferencia de zona*. Para permanecer sincronizado, los servidores de nombres secundarios consultan a los primarios regularmente (típicamente cada tres horas) y reejecutan la transferencia de zona si el primario ha sido actualizado. Un servidor de nombres puede operar como primario o secundario para múltiples dominios, o como primario para unos y secundario para otros. Un servidor primario o secundario realiza todas las funciones de un servidor caché.
- caché: un servidor de nombres que no tiene autoridad para ninguna zona se denomina servidor caché. Obtiene todos sus datos de servidores primarios o secundarios. Requiere al menos un registro NS (Servidor de Nombre) para apuntar a un servidor del que pueda obtener la información inicialmente.

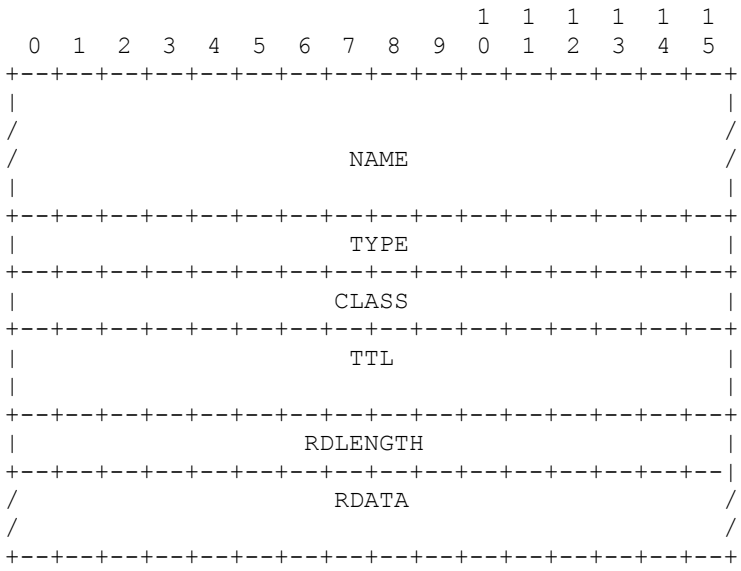
Cuando un dominio se registra en la raíz y se establece una zona de autoridad separada, se aplican las siguientes reglas:

- El dominio se debe registrar en el administrador de la raíz.
- Debe haber un administrador identificado para el dominio.
- Debe haber al menos dos servidores de nombres con autoridad para la zona que sean accesibles desde fuera y dentro del dominio para evitar cualquier posible punto débil.

También se recomienda que los servidores de nombres que delegan autoridad apliquen estas reglas, ya que son responsables del comportamiento de los servidores de nombres delegados.

2.3. Registros de recursos del DNS

La base de datos distribuida del DNS se compone de *RRs (registros de recurso o "resource records").* Estos proporcionan un mapeado entre nombres de dominio y *objetos de red*. Los objetos de red más comunes son las direcciones de los hosts, pero el DNS está diseñado para acomodarse a una variada gama de distintos objetos. El formato general del registro de recurso es:



NAME

Es el nombre del dominio al que se refiere el registro. El DNS es muy general en las reglas de composición de nombres de dominio. Un nombre de dominio consiste en una serie de etiquetas formadas por caracteres alfanuméricos o guiones, cada etiqueta con una longitud de 1 a 63 caracteres, comenzando con un carácter alfabético. Los nombres de domino se representan habitualmente separando las etiquetas mediante un punto. En los mensajes, cada etiqueta incluye un byte al principio indicando la longitud de esta etiqueta. Todos los nombres acaban con una etiqueta de longitud cero que indica el dominio raíz. Los nombres de dominio no son sensibles a mayúsculas y minúsculas.

CLASS

Identifica la familia del protocolo. La clase 1 (IN) se usa para Internet.

TYPE

Identifica el tipo de recurso del registro. El tipo 1 (A) identifica una dirección de host.

TTL

Es el *"time-to-live"* o tiempo en segundos que el registro será válido en la caché de un servidor de nombres. Se almacena en el DNS como un valor de 32 bits sin signo. 86400 (un día) es un valor típico para registros que apuntan a una dirección IP.

RDLENGTH

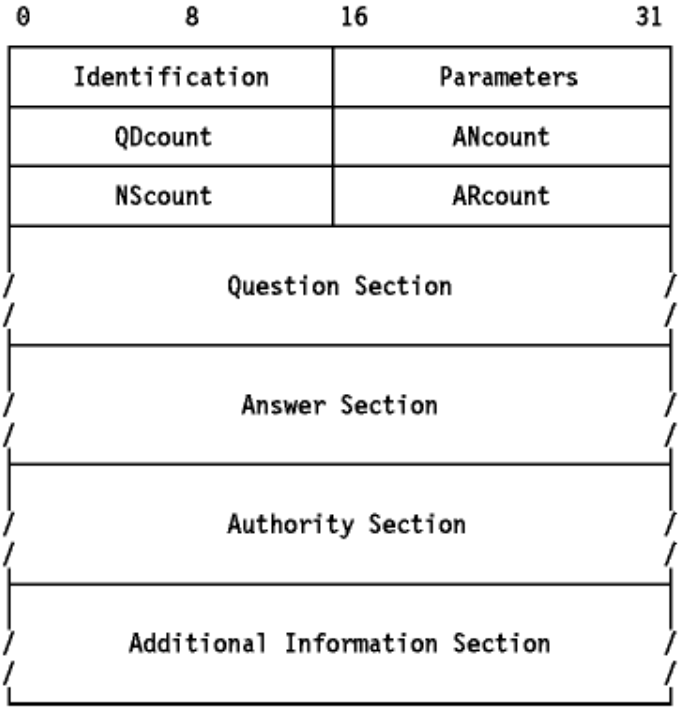
Longitud de la parte de datos.

RDATA

Datos del registro. En función del tipo y clase del registro los datos variarán. Así, por ejemplo, si el tipo es A y la clase IN, los datos serán cuatro bytes indicando una dirección IP.

2.4. Mensajes del DNS

Todos los mensajes del DNS utilizan un único formato:



El "resolver" envía la trama al servidor de nombres. Sólo la cabecera y la sección "question" se utilizan para la consulta. Las respuestas o retransmisiones de las consultas usan la misma trama, pero llenan más secciones de la misma (las secciones "answer/authority/additional").

a) *Formato de la cabecera*

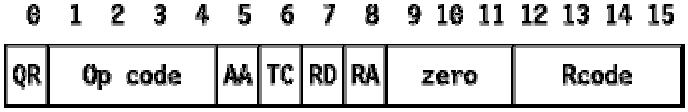
La sección de cabecera siempre ha de aparecer y tiene una longitud fija de 12 bytes. Las otras secciones son de longitud variable.

- ***ID (Identification)***

Un identificador de 16 bits asignado por el resolvedor. Este identificador se copia en la respuesta correspondiente del servidor de nombres y se puede usar para diferenciar respuestas cuando concurren múltiples consultas.

- ***Parameters***

Un campo de 16 bits con el siguiente formato:



QR

Flag que indica consulta (0) o respuesta (1).

Op code

Campo de 4 bits especificando el tipo de consulta:

- 0: consulta estándar (QUERY).
- 1: consulta inversa (IQUERY).
- 2: solicitud del estado del servidor(STATUS).

Se reservan los otros valores para su uso en el futuro.

AA

Flag de respuesta autoritativa. Si está activo en una respuesta, especifica que el servidor de nombres que responde tiene autoridad para el nombre de dominio enviado en la consulta.

TC

Flag de truncado. Activo si el mensaje es más largo de lo que permite el canal.

RD

Flag de recursividad. Este bit indica al servidor de nombres que se pide resolución recursiva. El bit se copia en la respuesta.

RA

Flag de recursividad disponible. Indica si el servidor de nombres soporta resolución recursiva.

zero

3 bits reservados para uso futuro. Deben ser cero.

Rcode

Código de respuesta de 4 bits. Posibles valores son:

- 0: Ningún error.
- 1: Error de formato. El servidor fue incapaz de interpretar el mensaje.
- 2: Fallo en el servidor. El mensaje no fue procesado debido a un problema con el servidor.
- 3: Error de nombre. El nombre de dominio de la consulta no existe. Sólo válido si el bit AA está activo en la respuesta.
- 4: No implementado. El tipo solicitado de consulta no está implementado en el servidor de nombres.
- 5: Rechazado. El servidor rechaza responder por razones políticas.

Los demás valores se reservan para su uso en el futuro.

- ***QDcount***

  Un entero sin signo de 16 bits que especifica el número de entradas en la sección "question".

- ***ANcount***

  Un entero sin signo de 16 bits que especifica el número de RRs en la sección "answer".

- ***NScount***

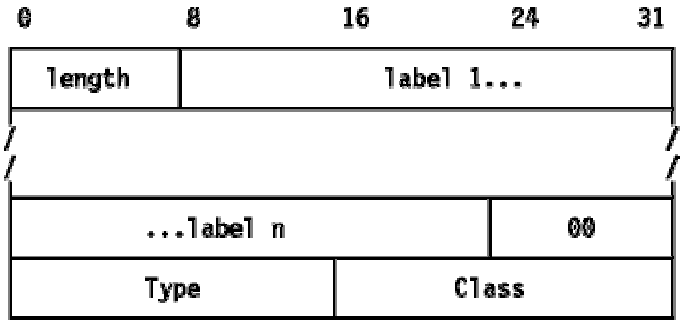
  Un entero sin signo de 16 bits que especifica el número de RRs en la sección "authority".

- ***ARcount***

  Un entero sin signo de 16 bits que especifica el número de RRs en la sección "additional records".

b) Sección "Question"

La siguiente sección contiene las consultas al servidor de nombres. Contiene QDcount (generalmente 1) entradas, cada una con el siguiente formato:



Todos los campos están alineados por bytes. La alineación del campo "Type" a 4 bytes es un ejemplo, y no es obligatoria en el formato.

- ***length***

  Un byte que indica la longitud de la siguiente etiqueta.

- ***label***

  Un elemento del nombre de dominio. El nombre de dominio se almacena como una serie de etiquetas de longitud variable, cada una precedida por un campo "length".

- ***00***

  Un valor de 00 indica el fin del dominio y representa la etiqueta nula del dominio raíz.

- ***Type***

  2 bytes especificando el tipo de consulta. Para consultas de direcciones se usa el valor 'A' (1).

- ***Class***

  2 bytes especificando la clase de consulta. Para consultas en Internet, se usa el valor 'IN' (1).

c) Secciones "Answer", "Authority" y "Additional Resource"

Estas tres secciones contienen un número variable de registros de recursos. El número se especifica en el campo correspondiente de la cabecera. El formato del registro de recursos se discute en el apartado 2.3.

d) Compresión de mensajes

Con el fin de reducir el tamaño del mensaje, se utiliza un esquema de compresión para eliminar la repetición de nombres de dominio en los diversos RRs. Cualquier dominio o lista de etiquetas duplicada se sustituye por un puntero a la ocurrencia anterior. El puntero tiene la forma de un campo de 2 bytes:

Los primeros 2 bits distinguen al puntero de una etiqueta normal, que está restringida a una longitud de 63 bytes más el byte de longitud.

El campo de 'offset' especifica un desplazamiento desde el comienzo el mensaje. Un 'offset' igual a cero especifica el primer byte del campo ID de la cabecera.

e) Transporte

Los mensajes DNS se transmiten como datagramas (UDP) o sobre un canal (TCP). En ambos casos, se usa como puerto destino de las peticiones DNS (puerto origen del servidor) el puerto 53.

Un resolvedor DNS o un servidor que envía una consulta que no supone una transferencia de zona *debe* enviar una consulta UDP primero. Si la sección "answer" de la respuesta está truncada y el solicitante soporta TCP, debería intentarlo de nuevo usando TCP. Se prefiere UDP a TCP para las consultas porque UDP tiene un factor de carga mucho menor, y su uso es esencial para un servidor fuertemente cargado. El truncamiento de mensajes no suele ser un problema dados los contenidos actuales de la base de datos del DNS, ya que típicamente se pueden enviar en un datagrama 15 registros, pero esto podría cambiar a medida que se añaden nuevos tipos de registro al DNS.

TCP debe usarse para actividades de transferencia de zonas debido a que el límite de 512 bytes de UDP siempre será inadecuado para una transferencia de zona.

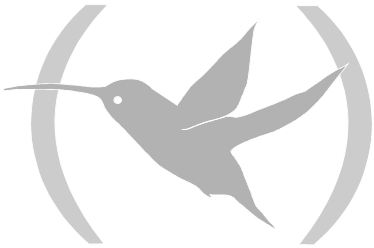
Los servidores de nombres deben soportar ambos tipos de transporte.

3. Referencias

RFC 1034
DOMAIN NAMES – CONCEPTS AND FACILITIES, P. Mockapetris, Noviembre 1987

RFC 1035
DOMAIN NAMES – IMPLEMENTATION AND SPECIFICATION, P. Mockapetris, Noviembre 1987

Capítulo 2
Configuración del DNS



1. Configuración del DNS

Para acceder al menú de configuración de los parámetros del cliente DNS, debe teclearse el comando **FEATURE DNS** desde el menú de configuración.

```
*P 4
User Configuration
Config>FEATURE DNS
-- DNS resolver user configuration --
DNS config>
```

Las opciones de este menú de configuración son las siguientes:

```
DNS config>?
LIST                    Displays the DNS configuration
N-RETRANSMISSIONS       Maximum number of DNS petition transmissions
NO
SERVER                  DNS name server to which the petitions are carried out
SOURCE-PORT             UDP port used as source in the DNS petitions
T-RETRANSMISSIONS       Time between DNS petition retransmissions
EXIT
```

1.1. LIST

Muestra configuración del DNS.

```
DNS config>LIST ?
ALL                     Displays the whole of the DNS configuration
N-RETRANSMISSIONS       Displays the maximum number of retransmissions
SERVERS                 Displays the IP addresses for the configured DNS servers
SOURCE-PORT             Displays the UDP port used as source
T-RETRANSMISSIONS       Displays the time between DNS petition retransmissions
DNS config>
```

a) LIST ALL

Muestra toda la configuración DNS.

```
DNS config>LIST ALL
Source port: 2658
Number of retransmissions: 5
Time between retransmissions: 1 sec
Name servers:
               172.24.0.6
               172.24.0.13
DNS config>
```

"Source port", puerto UDP usado como origen en las peticiones DNS.

"Number of retransmissions", número máximo de transmisiones de una petición DNS.

"Time between retransmissions", tiempo entre retransmisiones de una petición DNS.

"Name servers", direcciones IP de los servidores DNS configurados.

b) LIST N-RETRANSMISSIONS

Muestra el número de máximo de trasmisiones de una petición DNS.

```
DNS config>LIST N-RETRANSMISSIONS
Number of retransmissions: 5
DNS config>
```

c) *LIST SERVERS*

Muestra las direcciones IP de los servidores DNS configurados.

```
DNS config>LIST SERVERS
Name servers:
               172.24.0.6
               172.24.0.13
DNS config>
```

d) *LIST SOURCE-PORT*

Muestra el puerto UDP usado como origen en las peticiones DNS.

```
DNS config>LIST SOURCE-PORT
Source port: 2658
DNS config>
```

e) *LIST T-RETRANSMISSIONS*

Muestra el tiempo entre retransmisiones de una petición DNS.

```
DNS config>LIST T-RETRANSMISSIONS
Time between retransmissions: 1 sec
DNS config>
```

1.2. N-RETRANSMISSIONS

Configura el número de máximo de trasmisiones de una petición DNS.

```
DNS config>N-RETRANSMISSIONS
Maximum number of retransmissions (1-10)[5]? 3
DNS config>
```

1.3. NO

a) *NO SERVER*

Borra un servidor de nombres DNS configurado.

```
DNS config>NO SERVER
Name server ip address to delete [0.0.0.0]? 192.68.63.56
DNS config>NO SERVER
Name server ip address to delete [0.0.0.0]? 1.2.3.4
Name server not found
DNS config>
```

1.4. SERVER

Agrega un servidor de nombres DNS al que realizar las peticiones. En caso de haberse configurado el máximo número de servidores posible (actualmente tres), se indica con un mensaje de error.

```
DNS config>SERVER
Name server ip address [0.0.0.0]? 192.68.63.197
DNS config>
DNS config>SERVER
Maximum number of name servers already configured
DNS config>
```

1.5. SOURCE-PORT

Configura el puerto UDP usado como origen en las peticiones DNS.

```
DNS config>SOURCE-PORT
Source port[2658]? 2345
DNS config>
```

1.6. T-RETRANSMISSIONS

Configura el tiempo entre retransmisiones de una petición DNS.

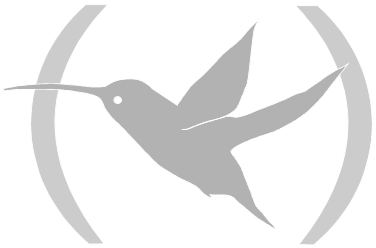
```
DNS config>T-RETRANSMISSIONS
Time between retransmissions (sec) (1-5 sg)[1]? 5
DNS config>
```

1.7. EXIT

Sale del menú de configuración del DNS.

```
DNS config>EXIT
Config>
```

Capítulo 3
Monitorización del DNS



1. Monitorización del DNS

Para acceder al menú de monitorización de los parámetros del cliente DNS, debe teclearse el comando **FEATURE DNS** desde el menú de monitorización global.

```
*P 3

+FEATURE DNS
-- DNS resolver user monitoring --
DNS>
```

Las opciones de este menú de monitorización son las siguientes:

```
DNS>?
LIST
LOOKUP
EXIT
DNS>
```

1.1. LIST

Muestra distintos parámetros del funcionamiento del DNS.

```
DNS>LIST ?
MEMORY-USED
LOOKUP-RESULTS
DNS>
```

a) LIST MEMORY-USED

Muestra los recursos de memoria en uso por el cliente DNS.

```
DNS>LIST MEMORY-USED

Memory in use: 0
DNS>
```

b) LIST LOOKUP-RESULTS

Muestra el resultado de las 10 últimas peticiones DNS realizadas desde monitorización (usando el comando LOOKUP)

```
DNS>LIST LOOKUP-RESULTS

Last DNS Lookup Queries
-----------------------
www.elmundo.es: IP addresses
    212.80.177.133
www.microsoft.com: Maximum number of retries reached
DNS>
```

1.2. LOOKUP

Realiza una petición DNS del nombre especificado. Cuando se resuelve la dirección, ésta aparece por pantalla. Mientras se resuelve la petición, la consola queda bloqueada. Si se desea terminar la petición DNS antes de que se resuelva, debe pulsarse Ctrl+C.

```
DNS>LOOKUP
Name  []? www.teldat.es
Press Ctrl+C to stop the query

172.24.0.56
DNS>
```

En caso de que la petición no se complete con éxito se indica con un mensaje significativo el tipo de error que se produjo.

```
DNS>LOOKUP
Name  []? www.microsoft.com
Press Ctrl+C to stop the query


DNS Error: Maximum number of retries reached
DNS>
```

1.3. EXIT

Sale del menú de monitorización del cliente DNS.

```
DNS>EXIT
+
```