UNIVERSITAT POLITÈCNICA DE VALÈNCIA

El formato de los mensajes DNS

Apellidos, nombre	Baydal Cardona, María Elvira (mebaydal@disca.upv.es)
Departamento	Informática de Sistemas y Computadores
Centro	Escola Tècnica Superior d'Enginyeria Informática

1 Resumen de las ideas clave

En este artículo vamos a explicar el formato de los mensajes que intercambian los servidores y clientes del servicio de nombres de dominio, conocido como DNS (*Domain Name System*). La descripción de estos mensajes nos permitirá interpretar las consultas y respuestas obtenidas al utilizar programas cliente DNS de nivel de usuario, como las órdenes *dig* y *host*, de las que veremos unos ejemplos de uso.

Para ello comenzaremos

2 Objetivos

Una vez que leas con detenimiento este documento, serás capaz de explicar cómo son los mensajes DNS y qué campos tienen, así como, el significado de cada campo. También podrás diferenciar los mensajes DNS de pregunta y de respuesta.

Además, podrás aplicar los conceptos anteriores de forma práctica interpretando los resultados de los clientes *dig* y *host* que te permitirán realizar consultas DNS.

3 Introducción

Para dominar un protocolo de red es necesario conocer el formato de los mensajes que utiliza. Eso nos ayuda a comprender mejor el funcionamiento del protocolo. Por ejemplo, sabemos que una de las principales funciones del servicio DNS es averiguar la dirección IP asociada a un nombre de dominio, pero ¿cómo pregunta el cliente esta información al servidor? Recuerda que esto corresponde a una consulta de tipo A. ¿Y cuando el cliente quiere averiguar el servidor SMTP asociado a un dominio de correo? Es decir una consulta de tipo MX, ¿utiliza otro formato de mensaje distinto? ¿Cómo responde el servidor a estas consultas? En este artículo daremos respuesta a estas cuestiones.

4 Desarrollo

Pasemos ya a describir el formato de los mensajes DNS.

La primera diferencia importante con otros protocolos tradicionales de aplicación como, por ejemplo, los de correo: SMTP, POP3 o los utilizados tradicionalmente en la web como HTTP 1.1, es que el formato de los mensajes DNS es binario. Aquí los mensajes intercambiados no son texto en formato ASCII y, por lo tanto, los usuarios no somos capaces de interpretar el contenido directamente.

Además, el formato de los mensajes de petición del cliente y de las respuestas del servidor es similar. Ambos incluyen una sección de cabecera, mostrada en la figura 1 en amarillo, y una sección de preguntas. Las 3 secciones últimas: respuestas, autoridad e información adicional sólo pueden aparecer en las respuestas y a veces no están, no son campos obligatorios.

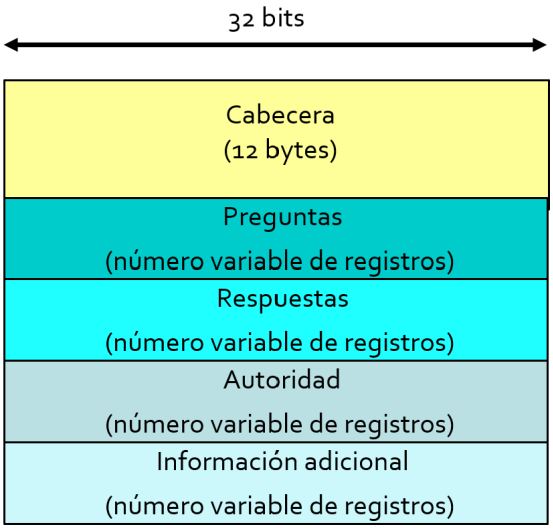

Figura 1. Campos de los mensajes DNS

4.1 Cabecera de los mensajes DNS

Empezaremos describiendo la cabecera del mensaje, que tiene longitud constante. En total 12 bytes, distribuidos en 6 campos de 2 bytes cada uno. Puedes ver la distribución de los campos de la cabecera en la (Figura 2).

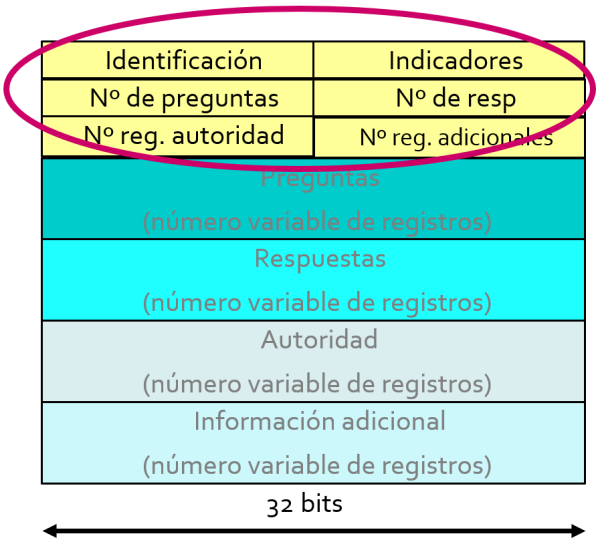

Figura 2. Campos de la cabecera de un mensaje DNS

El primer campo es un identificador que permite asociar las preguntas con sus respuestas. Al responder una pregunta se copia en la respuesta el valor del campo de identificación.

Los indicadores son varios bits que permiten distinguir diferentes condiciones del mensaje. Incluimos las siglas en inglés que los identifican porque son las que aparecen en los programas cliente que utilizaremos después.

- En primer lugar, el indicador "QR" (*QUERY*) indica si el mensaje es una pregunta o una respuesta. Paradójicamente este bit se activa en las respuestas.

- El bit “AA” (*AUTHORIZED ANSWER*) de respuesta autorizada, que tiene significado sólo en las respuestas, está activado cuando la respuesta proviene de un servidor autorizado del dominio.
- Mediante el bit “RD” (*RECURSION DESIRED*) de recursión deseada el cliente puede solicitar que el servidor realice una búsqueda recursiva si no dispone de la información que le solicita el cliente.
- El bit “RA” (*RECURSIÓN AVAILABLE*) de recursión disponible se activa si el servidor está dispuesto a utilizar recursividad. Por ejemplo, los servidores raíz nunca la permiten.

Los restantes campos de la cabecera indican el número de registros que se incluyen en las 4 secciones siguientes, que siguen a la cabecera, ya que pueden contener un número variable de registros. De estos campos, en los mensajes de consulta sólo el “número de preguntas” será distinto de cero, ya que el resto de campos están relacionados con la respuesta.

4.2 Secciones de preguntas, respuestas, autoridad e información adicional

Pasemos ahora a describir las 4 secciones siguientes de los mensajes DNS.

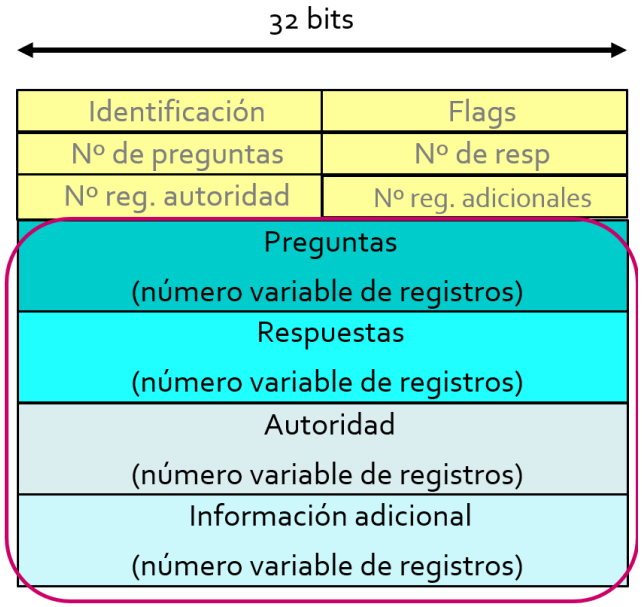

Figura 3. Secciones "Preguntas, Respuestas", "Autoridad" e "Información Adicional" de un mensaje DNS

La sección “Preguntas” incluye la consulta a realizar, indicando el tipo de registro solicitado y su nombre. Esta sección se copia en el mensaje de respuesta que devuelve el servidor. Habitualmente sólo se envía una pregunta. Por ejemplo, si buscamos la dirección IP de un host preguntaremos por un registro de tipo A y daremos el nombre del host, como podemos ver en la figura 3 donde se ha utilizado el nombre de dominio www.upv.es.

```
;; ->>HEADER<<- opcode: NOT QUERY, status: NOERROR, id: 53576
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;www.upv.es.                IN    A
```

Figura 4. Cabecera y sección "Preguntas" de un mensaje DNS (obtenido mediante la orden Linux dig)

En la sección “Respuestas” el servidor DNS devuelve el registro completo solicitado. Por ejemplo, en el caso anterior nos devolvería la dirección IP asociada al nombre de dominio indicado. Al devolvernos el registro completo también se incluyen aquí los campos nombre, tipo de registro, y el tiempo de vida que puede mantenerse el registro en caché. Esta sección puede incluir varios registros, por ejemplo, porque el nombre indicado tenga varias direcciones IP asociadas o por otros motivos.

La sección “Autoridad” contiene registros de tipo NS con los nombres de servidores DNS autorizados para el dominio DNS. Recuerda que los registros de tipo NS incluyen un nombre de dominio y el nombre de un servidor DNS autorizado para ese dominio. Sin embargo, la dirección IP del servidor DNS estará en un registro de tipo A o AAAA, y no forma parte del registro NS. Por este motivo, la sección “Información adicional” permite mejorar la eficiencia del servicio incluyendo esta información adicional sobre la dirección IP que posiblemente el cliente podría pedir a continuación. Es frecuente, por ejemplo, si se envía información en la sección “Autoridad” incluir aquí registros de tipo A o AAAA con las direcciones IP de los servidores de nombres del dominio.

Podemos ver todo esto mejor mediante el ejemplo en la sección siguiente.

4.3 Ejemplo de consulta DNS utilizando el cliente dig

Normalmente las consultas DNS son gestionadas directamente por los programas de aplicación como apoyo para realizar su tarea y sin intervención del usuario. Por ejemplo, cuando indicamos el nombre de un servidor web en un navegador, el primer paso será obtener la dirección IP del servidor mediante una consulta DNS. Lo mismo ocurre cuando un cliente de correo debe conectar con un servidor SMTP. Sin embargo, todos los sistemas operativos proporcionan, además, diferentes clientes DNS que pueden ser ejecutados directamente por los usuarios, habitualmente mediante órdenes del sistema operativo. Uno de los más sencillos es la orden “dig”, disponible en sistemas Unix y derivados como Linux o IOS. Es el que utilizaremos para realizar nuestro ejemplo.

Por defecto en este tipo de clientes DNS cuando el usuario no especifica el tipo de consulta se asume que es de tipo A (*Address*), como podemos ver en la Figura 5. Intenta interpretar el tipo de pregunta que hemos hecho y de respuesta que hemos obtenido, analizando la cabecera y las distintas secciones (*Question, Answer, Authority* y *Additional*), antes de seguir leyendo.

```
redes12@zoltar:~/Escritorio$ dig ias.cc.upv.es
; <<>> DiG 9.7.0-P1 <<>> www.upv.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53576
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 6

;; QUESTION SECTION:
;ias.cc.upv.es.                 IN      A

;; ANSWER SECTION:
ias.cc.upv.es.          10800   IN      A       158.42.4.23

;; AUTHORITY SECTION:
upv.es.                 10800   IN      NS      mirzam.ccc.upv.es.
upv.es.                 10800   IN      NS      chico.rediris.es.
upv.es.                 10800   IN      NS      sun.rediris.es.
upv.es.                 10800   IN      NS      vega.cc.upv.es.

;; ADDITIONAL SECTION:
mirzam.ccc.upv.es.      10800   IN      A       158.42.1.5
vega.cc.upv.es.         10800   IN      A       158.42.4.1
sun.rediris.es.         2665    IN      A       130.206.1.2
sun.rediris.es.         5364    IN      AAAA    2001:720:418:caf1::2
chico.rediris.es.       2669    IN      A       130.206.1.3
chico.rediris.es.       4607    IN      AAAA    2001:720:418:caf1::3

;; Query time: 2 msec
;; SERVER: 158.42.249.8#53(158.42.249.8)
```

Consulta Tipo A implícita

cabecera

Las respuestas incluyen el tipo de registro y el TTL en s

Figura 5. Ejemplo de respuesta DNS obtenido mediante la orden "dig"

En este ejemplo, al hacer una consulta de tipo A, mediante la orden “dig ias.cc.upv.es”, estamos preguntando cuál es la dirección IP asociada al nombre ias.cc.upv.es.

Analicemos ahora el contenido de la respuesta obtenida. La respuesta incluye, en primer lugar, la cabecera con los indicadores:

- El bit “QR” (QUERY) que al estar activado indica que estamos viendo una respuesta (es un poco mentiroso el DNS 😉).
- El siguiente bit “AA” (*AUTHORIZED ANSWER*) indica que es una respuesta autorizada. Es decir que la información proviene de un servidor DNS autorizado para el dominio upv.es.
- Los indicadores “RD” (*RECURSION DESIRED*) y “RA” (*RECURSION AVAILABLE*) nos muestran que el cliente ha solicitado recursión y el servidor que responde, que es el servidor local del cliente (158.42.249.8), le indica que la tiene disponible.

Los 4 últimos campos de la cabecera indican el número de registros en las secciones siguientes: 1 registro de pregunta, 2 registros de respuesta, 4 registros de autoridad y 6 registros de información adicional.

Como ya hemos dicho, la pregunta es de tipo A (*Address*) y el campo nombre del registro es www.upv.es, y queremos obtener el campo valor de este registro.

En los registros de respuesta se indica que el nombre ias.cc.upv.es tiene asociada la dirección IP 158.42.4.23.

En los registros de autoridad podemos ver 4 registros NS (*Name Server*) que contienen nombres de servidores de nombres autorizados para el dominio upv.es.

Finalmente, la sección de información adicional contiene registros de tipo A y AAAA con las direcciones IPv4 e IPv6, respectivamente, de los servidores de nombres anteriores.

Podemos ver también que todas las secciones incluyen el tiempo de vida de los registros, expresado en segundos, lo que permite almacenar esos registros en la caché DNS del ordenador cliente y del servidor DNS local que le está devolviendo la respuesta, durante el tiempo indicado. Si el TTL fuese 0 la respuesta no se podría guardar en caché, y habría que volver a preguntar cada vez que se necesitase de nuevo.

4.4 Ejercicio propuesto

Después de leer la explicación del ejercicio anterior, ahora deberías intentar interpretar tú esta nueva consulta de la figura 6 sin problemas. La hemos realizado mediante otro cliente DNS de Linux, la orden **host**, también muy sencillo de manejar. Al incluir la opción –v el programa muestra información más detallada del mensaje de respuesta DNS.

```
Rdc12:~redes12$ host -t NS -v upv.es
Trying "upv.es"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12556
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;upv.es.                IN  NS

;; ANSWER SECTION:
upv.es.          874  IN  NS  chico.rediris.es.
upv.es.          874  IN  NS  vega.cc.upv.es.
upv.es.          874  IN  NS  mirzam.ccc.upv.es.
upv.es.          874  IN   NS   sun.rediris.es.

Received 117 bytes from 192.168.0.1#53 in 61 ms
```

Figura 6. Consulta DNS mediante la orden "host"

Responde a las cuestiones siguientes:

1. Indica qué flags están activados en el mensaje DNS y su significado.
2. ¿Qué tipo de consulta hemos realizado? ¿Qué estamos intentando obtener?
3. Explica la información qué hemos obtenido en la sección de respuesta.
4. Indica cómo obtendrías la dirección IP el servidor DNS "chico.red.iris.es" mediante las órdenes **host** y **dig**, alternativamente desde Microsoft Windows puedes emplear el cliente **nslookup**. ¿En qué sección nos hubieran podido incluir la información con la dirección IP del servidor DNS en el mensaje de la figura 6? ¿Qué tipo de registro hubiese sido necesario incluir?

SOLUCIÓN

1. El mensaje lleva activados los bits de la cabecera QR, que indica que se trata de una respuesta, RD, porque se ha solicitado recursión y RA, porque el servidor consultado acepta consultas recursivas.
2. El tipo de consulta que hemos solicitado es NS (*Name Server*), lo que hemos indicado mediante la opción –t. Como ves, además de la sección de pregunta, ahora tenemos 4 registros de respuesta pero no nos han devuelto registros de autoridad ni de información adicional.

3. La sección de respuesta nos devuelve los nombres de dominio de 4 servidores DNS que atienden el dominio upv.es.
4. La dirección IP del servidor "chico.red.iris.es" y del resto de servidores DNS se podía haber enviado en la parte de información adicional mediante registros de tipo A o AAAA, dependiendo del tipo de direcciones IP que tengan asignadas. Si no se hubiese devuelto esa información adicional, probablemente el cliente la hubiese solicitado a continuación. Nosotros como usuarios la podemos solicitar en Linux con las órdenes "host -t A chico.rediris.es" o "dig chico.rediris.es" o en Microsoft Windows con la orden "nslookup chico.rediris.es".

5 Resumen

Para terminar, resumiremos los contenidos que hemos visto en este artículo. Hemos explicado que los mensajes DNS pueden ser de dos tipos: pregunta o respuesta. Ambos con la misma estructura: una cabecera y varias secciones a continuación, de las cuales sólo la primera, la sección de preguntas es obligatoria. De hecho, los mensajes de tipo pregunta solo incluyen la cabecera y la sección de preguntas.

También hemos visto dos ejemplos prácticos realizando consultas DNS mediante las órdenes "dig" y "host" de Linux.

6 Bibliografía

Kurose, J.F.; Ross, K.W.: "Redes de computadoras. Un enfoque descendente", en Ed. Pearson, 2017, pág. 112-116.

Mockapetris, P. "RFC 1034. DOMAIN NAMES - CONCEPTS AND FACILITIES", 1987. Disponible en https://www.ietf.org/rfc/rfc1034.txt.