ADMINISTRACIÓN DE REDES Y SISTEMAS

PRÁCTICAS DE LABORATORIO

Servicio de nombres de dominio DNS

El DNS es un servicio fundamental, ya que prácticamente cualquier aplicación de red en algún momento va necesitar traducir un nombre de red a una dirección de red. Además, a lo largo de los años se ha ido aprovechando la infraestructura del DNS para guardar otra información para diversos servicios. Por ejemplo, el DNS contiene información esencial para encaminar los correos electrónicos.

La información del DNS es esencialmente pública y se organiza como un árbol jerárquico de dominios, cuya información se encuentra segmentada en zonas y distribuida por millones de servidores de DNS por toda la Internet. El propietario de cada dominio decide qué quiere publicar en su rama del DNS. Para su buen funcionamiento se usan mecanismos descentralizados con protocolos estandarizados que requieren escasa compenetración entre las partes.

En esta práctica se trabajará con el paquete de software ISC BIND, que es una de las implementaciones de cliente y servidor de DNS más utilizadas en el mundo POSIX.

Conceptos básicos del DNS

En clase se repasarán los conceptos básicos del DNS, tales como características, propósito, arquitectura, componentes, búsquedas, tipos de registros, replicación, vistas, etc. Muchos de estos conceptos ya se han tratado en asignaturas anteriores. A medida que se van repasando, se hará uso frecuente del programa drill para conocer mejor el funcionamiento del DNS y como herramienta de diagnóstico. Otras herramientas similares son dig y nslookup.

Tarea 1: Utilice drill para consultar registros, realizar búsquedas descendentes, entender las respuestas obtenidas, etc. En el apéndice I de este enunciado tiene un resumen del uso de drill.

Configuración de ISC BIND como servidor de resolución

Hasta ahora todos sus sistemas han estado usando como servidor de resolución local a un servidor del laboratorio (probablemente 10.49.8.100, aunque también podría haber sido alguno del tipo 8.8.8.8, 1.1.1.1, etc.).

En este apartado vamos a instalar y usar nuestro propio servidor de resolución. Para ello se instalará BIND en una de las máquinas del alumno y se hará que las demás lo usen como servidor de resolución.

Tarea 2: Instale ISC BIND 9.16 (`pkg install bind916`) en el sistema 02.

Tarea 3: Revise la configuración por defecto que aparece en el fichero `/usr/local/etc/namedb/named.conf`. Para actuar como servidor de resolución no hace falta modificar nada, salvo que la opción `listen-on` indica que solo escuche en la interfaz local, por lo que tendrá que cambiarla para poder atender a otros sistemas.

Tarea 4: Habilite el arranque automático del servicio (`sysrc named_enable=YES`). Después, arranque el servicio (`service named start`).

NOTA: cada vez que modifique la configuración o los ficheros de zona de su servidor de DNS debe indicarle que incorpore los cambios mediante un mandato como `service named reload` o `rndc reload`. Para detectar posibles errores de configuración, ejecute primero `named-checkconf`.

Tal como se instala, ISC BIND ya funciona como servidor de resolución, en concreto como servidor caché que hace búsquedas descendentes partiendo del dominio raíz.

Tarea 5: Utilice `drill` desde diversos sistemas para verificar que el servidor que acaba de instalar es capaz de resolver consultas de dominios cualesquiera del DNS mundial (tendrá que usar @ para que `drill` envíe las preguntas a su servidor de DNS).

Tarea 6: (Opcional) Habilite el registro detallado de eventos del servidor de DNS según lo que se indica en el Moodle de la asignatura. Utilícelo para obtener información más detallada sobre la actividad del servidor de DNS.

Los sistemas de su red corporativa hasta ahora han utilizado a un servidor de DNS del laboratorio para hacer consultas al DNS. Como ya disponemos de nuestro propio servidor de resolución, vamos a utilizarlo en los sistemas internos.

Tarea 7: Configure su DHCP para que indique a los clientes que usen como servidor de resolución de DNS al servidor que acaba de instalar. Después compruebe que las consultas de DNS funcionan con normalidad en los sistemas de su red corporativa.

Observe que, si lo desea, puede usar como servidor de resolución al servidor de DNS de cualquier otro compañero del laboratorio. En general, no conviene que un servidor de resolución atienda a cualquier cliente, ya que ello puede conllevar a un abuso de recursos y problemas de seguridad. Existen diversas maneras de establecer un control de acceso, y en esta práctica se va a utilizar la más básica, que consiste en comprobar la dirección de red del cliente.

Tarea 8: Configure a su servidor de DNS para que solo admita consultas de resolución provenientes de los equipos que usted controla, es decir, de su red corporativa (tendrá que usar `acl`, `allow-query`, `allow-recursion`).

Hasta aquí el servidor de resolución hacía las búsquedas completas a partir de la raíz, pero también se puede hacer que se apoye en otro servidor de resolución (es lo que en inglés se denomina *forwarding*).

Tarea 9: Configure su servidor de DNS para que reenvíe las consultas al servidor de resolución del laboratorio (10.49.8.100) o, si lo prefiere, en algún otro público de Internet, como 8.8.8.8, 1.1.1.1, etc. Compruebe que las consultas de DNS continúan funcionando correctamente en los sistemas de su red corporativa.

Registro de un dominio y delegación en un servidor autoritativo

Para tener presencia digital, un requisito básico es tener uno o varios dominios de DNS que permitan publicar los nombres que permitirán que los clientes, usuarios, etc. lleguen a nuestros servicios.

El primer paso consiste en reservar los dominios deseados a través de algún agente registrador; por ejemplo, para reservar dominios bajo `.es` se puede usar cualquiera de los agentes registradores autorizados por dominios.es, que es el responsable de la gestión del TLD .es. Esta operación tiene un coste económico inicial y un coste de mantenimiento anual, generalmente en el entorno de unas pocas decenas de euros. Muchos agentes registradores también permiten reservar dominios bajo otros muchos TLD, si bien en algunos dominios nacionales puede ser necesario satisfacer requisitos especiales, como ser residente del país.

En el entorno del laboratorio se dispone de un agente registrador que permite reservar y delegar dominios bajo `mucs.es`. El registrador se encuentra en https://panel.mucs.es. Los dominios reservados en este registrador tienen un propósito meramente didáctico y en principio no serán visibles para la Internet mundial, ya que sus servidores autoritativos van a estar en sistemas del laboratorio que no están accesibles desde fuera de los laboratorios.

Tarea 10: Acceda al registrador y registre un dominio de su elección.

A continuación, se va a desplegar un servidor de DNS para almacenar en él la información de dicho dominio y delegar en él la autoridad sobre el mismo.

Tarea 11: Instale el paquete ISC BIND 9.16 (`pkg install bind916`) en el sistema 01. Haga que escuche en todas las interfaces (opción `listen-on`). Habilite su arranque automático (`sysrc named_enable=YES`). Después, arranque el servicio (`service named start`). Opcionalmente, habilite el registro detallado de actividad.

Tarea 12: Configure a este servidor de DNS para que actúe como servidor primario del dominio que ha registrado. Para ello tiene que generar un fichero de zona con los registros que desee publicar para su dominio y definir un bloque `zone` en la configuración del servidor de DNS.

Notas:

- Utilice frecuentemente los programas `named-checkconf` y `named-checkzone` para comprobar la validez de la configuración y del fichero de zona[1].
- Asegúrese de incrementar el número de serie del registro SOA cada vez que cambia algo en el fichero de zona.

[1] Como siempre, recuerde que una cosa es que una configuración o un fichero de zona sean válidos sintácticamente y otra cosa es que realmente sean correctos para lo que se pretende conseguir.

- Asegúrese de utilizar valores bajos en los TTL de su zona (del orden de 1 minuto). Esto sirve para que, si publica registros erróneos, desaparezcan rápidamente de las cachés de otros servidores del laboratorio.
- Revise el fichero `/var/log/messages` con frecuencia, ya que ahí aparecerán los posibles mensajes de error que produzca el servidor si hay errores en el fichero de zona.

Tarea 13: Utilice drill con la opción @ para hacer consultas directas a su servidor autoritativo y compruebe que las respuestas son acorde a lo esperado.

Tarea 14: Una vez esté convencido de que su servidor de DNS responde correctamente a las consultas sobre el dominio de su propiedad, delegue en él la autoridad sobre el mismo a través del panel de control del registrador. Después, compruebe que puede resolver nombres de su dominio con normalidad (es decir, sin forzar con @), tanto desde sus propios equipos, como desde cualquier otro equipo del laboratorio.

NOTA: observe que para realizar la tarea anterior no hace falta cambiar el servidor de DNS configurado para los clientes de DHCP.

Tarea 15: Desde un equipo externo a su red corporativa, haga una consulta a un registro cualquiera de su dominio. A continuación, modifique el valor del registro en cuestión y repita la consulta anterior. Si hace la modificación y la posterior consulta lo suficientemente rápido, debería observar que el registro en cuestión continúa con el valor antiguo. ¿Por qué? ¿Cuándo se verá el cambio que acaba de hacer?

Tarea 16: Haga lo mismo que en la cuestión anterior, pero en este caso con un registro que inicialmente no existe (aquí se trata de observar la caché de respuestas negativas).

El rol de servidor autoritativo del dominio de una organización es completamente independiente del rol de servidor de resolución para los equipos de la organización. De hecho, en las tareas anteriores hemos usado un servidor de DNS diferente para cada rol. Pero en adelante, y por conveniencia, vamos a unificar ambos roles en el servidor de DNS del sistema 01 (que también actúa como encaminador y servidor de DHCP). En los entornos reales esto puede que no siempre se haga así, ya que el servidor autoritativo está expuesto a la Internet en general, mientras que el servidor de resolución normalmente solo se utiliza desde una red corporativa.

Tarea 17: Configure su DHCP para que indique a los clientes que usen como servidor de resolución al servidor de DNS de su encaminador. Después compruebe que pueden resolver consultas de DNS en general sin problemas.

Tarea 18: Configure a su encaminador para que se use a sí mismo como servidor de resolución de DNS (`/etc/resolv.conf` o `/etc/dhclient.conf`, según como se configure la red en su encaminador).

Tarea 19: (Opcional) Configure el control de acceso en su servidor de DNS para que solo permita consultas recursivas a los clientes de su red corporativa. Si lo prefiere, puede demorar esta tarea hasta completar la configuración de vistas del siguiente apartado.

Vistas

En algunos casos de uso, bastante frecuentes, se desea que un servidor de DNS responda de manera diferente según de dónde venga la consulta. Por ejemplo, quizá a los clientes corporativos se les traduzcan ciertos registros que no se desea publicar para la Internet en general. O quizá a las consultas desde redes públicas se responda con direcciones públicas y a las consultas desde redes privadas corporativas se responda con direcciones privadas. Esto se puede conseguir por medio del uso de vistas.

Tarea 20: Defina dos vistas en su servidor de DNS, una para los clientes externos y otra para los clientes de la red corporativa y el propio encaminador.

Notas:

- Al definir vistas, todos los bloques `zone` han de estar dentro de alguna vista. Esto es aplicable también a los bloques `zone` que vienen predefinidos en la configuración del servidor de DNS. Piense si estos bloques predefinidos han de meterse en ambas vistas o solo en una de ellas.
- Revise los controles de acceso (sentencias `acl` y `allow-xxx`) para que haya los correctos en cada una de las vistas.

Zonas para traducción inversa

Si su organización tiene asignada la gestión de un bloque de direcciones IP, entonces puede que le interese habilitar la correspondiente zona para traducción inversa de esas direcciones IP. Para las direcciones públicas esto generalmente cae bajo la responsabilidad del proveedor de conexión a la red; en cambio, la gestión de las direcciones privadas por definición corresponde al que las usa.

En el laboratorio, las direcciones de la red externa (10.48/15) son gestionadas por el departamento y la traducción inversa de las mismas se gestiona en los servidores de DNS del laboratorio. En cambio, las direcciones de su red corporativa (172.x.y.z) son enteramente de su responsabilidad. Por tanto, para hacer una gestión más completa vamos a definir una zona de traducción inversa para dichas direcciones.

Tarea 21: Añada a su servidor de DNS lo necesario para que admita la traducción inversa de las direcciones IP que utiliza en su red corporativa. Tendrá que añadir un bloque `zone` y su correspondiente fichero de zona. Piense si hay que añadir la zona para traducción inversa en ambas vistas o solo en una de ellas.

Comprobaciones de funcionamiento esenciales

Para evitar anomalías en las actividades del laboratorio de los temas posteriores es esencial que verifique que todos sus sistemas pueden usar el servicio de DNS correctamente. Para ello, asegúrese de que en todos los cruces de esta tabla obtiene resultados correctos si hace consultas de DNS con `drill` (sin usar @ en ningún caso).

	Encaminador	Máquina externa	Máquina interna
Consulta al DNS mundial			
Consulta a su dominio			
Traducción inversa de sus direcciones privadas			

Replicación de zonas primario-secundario (opcional)

Dada la relevancia del servicio de DNS para la presencia digital de una organización, es fundamental que esté disponible en todo momento. De hecho, en el mundo real se requiere desplegar al menos dos servidores autoritativos para cualquier dominio.

En este apartado se va a desplegar un segundo servidor de DNS autoritativo para el dominio registrado por el alumno.

Tarea 22: Partiendo del ISC BIND que ya tiene instalado en el sistema 02, configúrelo para que actúe como servidor secundario (o esclavo) de su dominio. Para ello, en el primario tendrá que permitir las transferencias de zona desde el secundario y en el secundario tendrá que añadir el correspondiente bloque `zone` y definir cuál es el servidor primario.

Notas:

- El servidor secundario se va a usar exclusivamente como servidor autoritativo del dominio, por lo que no debe admitir consultas recursivas de ningún tipo.
- En el servidor secundario hay que especificar un nombre para el fichero de zona, pero no hay que rellenarlo ni copiarlo a mano. Se rellenará automáticamente en cuanto se descargue la zona del primario.
- El servidor primario tiene varias vistas y varias zonas. Piense si en el servidor secundario se necesitan vistas y cuáles de las zonas hay que replicar desde el primario.

Tarea 23: Añada, modifique o elimine registros en el primario y compruebe que los cambios se reflejan inmediatamente en el secundario (use `drill` con `@` para consultar al primario y al secundario). Observe que es fundamental incrementar el número de serie de la zona cada vez que se hace un cambio.

Tarea 24: Una vez esté convencido de que su servidor de DNS secundario se replica correctamente con el primario, añádalo como servidor delegado a través del panel de control del registrador. Compruebe que se pueden seguir resolviendo nombres de su dominio con normalidad con que solo uno de los dos servidores autoritativos esté levantado. Obviamente, si detiene el servidor primario los clientes de la red corporativa no podrán resolver ningún nombre de DNS, ya que en nuestro entorno ese servidor también actúa como servidor de resolución para dichos clientes.

APÉNDICE I: uso general de drill

Este apéndice explica el uso general de la herramienta drill para hacer consultas y diagnósticos del servicio de DNS, en base a varios ejemplos.

En primer lugar se muestra una consulta básica de un registro existente:

```
$ drill www.upm.es
1: ;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 5453
2: ;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
   0
3: ;; QUESTION SECTION:
4: ;; www.upm.es. IN    A

5: ;; ANSWER SECTION:
6: www.upm.es.    8474  IN    A     138.100.200.6

7: ;; AUTHORITY SECTION:

8: ;; ADDITIONAL SECTION:

9: ;; Query time: 44 msec
10:   ;; SERVER: 10.49.8.100
11:   ;; WHEN: Wed Dec 18 11:48:58 2019
12:   ;; MSG SIZE  rcvd: 44
```

A continuación se explican los aspectos más relevantes de la respuesta obtenida:

La línea 10 indica cuál es el servidor de DNS al que drill hizo la consulta. Por defecto, es el servidor de DNS del sistema (también llamado servidor local), el cual normalmente se habrá obtenido mediante DHCP en el arranque de la máquina. En algunos ejemplos posteriores se muestra cómo se puede indicar a drill que haga la consulta a un servidor de DNS específico.

El apartado “QUESTION SECTION” (líneas 3 y 4) indica qué es lo que drill ha preguntado al servidor de DNS. Como se puede observar, el tipo de registro por defecto es A y la clase por defecto es IN. En algunos ejemplos posteriores se muestra cómo se puede indicar a drill que busque un tipo de registro diferente.

Las líneas 1 y 2 contienen un resumen del resultado obtenido. El código de resultado (rcode, línea 1) indica que no hubo error (NOERROR). La línea 2 indica que se ha obtenido 1 registro de respuesta, 0 registros de autoridad y 0 registros adicionales. El valor de flags (línea 2) también es importante, y en este caso nos vamos a fijar en que aparece el flag ra (*recursión available*), que indica que el servidor de DNS nos permite hacerle consultas recursivas.

El apartado “ANSWER SECTION” (líneas 5 y 6) contiene los registros obtenidos como respuesta. En la respuesta se puede observar el TTL restante para este registro (8474 segundos) en la caché del servidor al que se hizo la pregunta.

Los apartados “AUTHORITY SECTION” y “ADDITIONAL SECTION” contienen los registros de autoridad y adicionales que vengan en la respuesta. En este ejemplo no venía ninguno.

 El siguiente ejemplo ilustra algunos aspectos adicionales:

```
$ drill mx etsist.upm.es
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 64407
;; flags: qr rd ra ; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 1
;; QUESTION SECTION:
;; etsist.upm.es. IN    MX

;; ANSWER SECTION:
etsist.upm.es.    86400 IN    MX    90 relay4.upm.es.
etsist.upm.es.    86400 IN    MX    100 relay.upm.es.
etsist.upm.es.    86400 IN    MX    10 smtp.etsist.upm.es.

;; AUTHORITY SECTION:
upm.es.     6069  IN    NS    chico.rediris.es.
upm.es.     6069  IN    NS    galileo.ccupm.upm.es.
upm.es.     6069  IN    NS    sun.rediris.es.
upm.es.     6069  IN    NS    einstein.ccupm.upm.es.

;; ADDITIONAL SECTION:
smtp.etsist.upm.es.     84436 IN    A     138.100.52.110

;; Query time: 3 msec
;; SERVER: 10.49.8.100
;; WHEN: Wed Dec 18 12:28:41 2019
;; MSG SIZE  rcvd: 210
```

En primer lugar, en la consulta se ha especificado un tipo de registro particular (MX).

En segundo lugar, en la respuesta han venido bastantes más registros que en el ejemplo anterior. En concreto, han venido 3 registros de respuesta, 4 de autoridad y 1 adicional. Cada uno de ellos tiene su TTL en la caché del servidor que proporcionó la respuesta.

Los registros extra (autoridad y adicionales) no responden a la consulta específica que se hizo, pero los servidores de DNS pueden añadirlos a la respuesta si disponen de esa información y consideran que puede ser útil al cliente que hizo la consulta.

 En este ejemplo se hace una consulta de un registro que no existe:

```
$ drill noexiste.mucs.es
;; ->>HEADER<<- opcode: QUERY, rcode: NXDOMAIN, id: 18285
;; flags: qr rd ra ; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;; noexiste.mucs.es.    IN    A

;; ANSWER SECTION:

;; AUTHORITY SECTION:
mucs.es.    15    IN    SOA   ns1.mucs.es. hostmaster.mucs.es.
2019025197 900 120 604800 15

;; ADDITIONAL SECTION:

;; Query time: 87 msec
```

```
;; SERVER: 10.49.8.100
;; WHEN: Wed Dec 18 12:38:30 2019
;; MSG SIZE  rcvd: 85
```

Se sabe que el registro no existe porque el código de resultado es NXDOMAIN. Además, como cabía esperar no viene ningún registro de respuesta, aunque sí viene el registro SOA de la zona, en el cual merece la pena destacar el TTL de la respuesta negativa (15 segundos en este caso) que resta en la caché del servidor que proporcionó la respuesta.

A veces, las consultas de registros que no existen devuelven una respuesta un poco diferente. Por ejemplo, en este caso:

```
$ drill noexiste.upm.es
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 56562
;; flags: qr rd ra ; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;; noexiste.upm.es.     IN    A

;; ANSWER SECTION:

;; AUTHORITY SECTION:
upm.es.     3600  IN    SOA   einstein.ccupm.upm.es. hostmaster.upm.es.
2019112502 86400 7200 1209600 3600

;; ADDITIONAL SECTION:

;; Query time: 5 msec
;; SERVER: 10.49.8.100
;; WHEN: Wed Dec 18 12:37:42 2019
;; MSG SIZE  rcvd: 95
```

Obsérvese que el código de resultado es NOERROR y hay 0 registros de respuesta. Esto denota que el registro concreto pedido no existe, pero que sí hay algún otro registro con el mismo nombre, pero distinto tipo. Puede comprobar que es así si hace la siguiente consulta: `drill –t ANY noexiste.upm.es`.

El siguiente ejemplo muestra cómo se puede hacer una consulta a un servidor de DNS específico. En concreto, se va a consultar el registro A www.upm.es a uno de los servidores autoritativos del dominio. En uno de los ejemplos anteriores aparecían dichos servidores y se va a preguntar a chico.rediris.es:

```
$ drill @chico.rediris.es www.upm.es
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 64198
;; flags: qr aa rd ; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4
;; QUESTION SECTION:
;; www.upm.es.    IN    A

;; ANSWER SECTION:
www.upm.es. 86400 IN    A     138.100.200.6

;; AUTHORITY SECTION:
upm.es.     86400 IN    NS    galileo.ccupm.upm.es.
upm.es.     86400 IN    NS    chico.rediris.es.
```

```
upm.es.     86400 IN    NS    sun.rediris.es.
upm.es.     86400 IN    NS    einstein.ccupm.upm.es.

;; ADDITIONAL SECTION:
sun.rediris.es.   28800 IN    A     199.184.182.1
sun.rediris.es.   7200  IN    AAAA  2620:171:808::1
chico.rediris.es. 28800 IN    A     130.206.1.3
chico.rediris.es. 7200  IN    AAAA  2001:720:418:caf1::3

;; Query time: 4 msec
;; SERVER: 130.206.1.3
;; WHEN: Wed Jan 15 12:47:07 2020
;; MSG SIZE  rcvd: 229
```

Lo más interesante de esta respuesta es que es autoritativa, a diferencia de todas las de los ejemplos anteriores. Esto se ve porque en la respuesta viene activado el flag aa (*authoritative answer*). Además, los TTL de los registros para los que este servidor tiene autoridad son siempre el TTL inicial (si se repite la consulta siempre viene el mismo valor de TTL, mientras que en los ejemplos anteriores el valor de TTL iba descendiendo).

En la respuesta anterior también se puede ver que el servidor de DNS no nos acepta consultas recursivas. Si intentamos alguna, se obtiene un rechazo:

```
$ drill @chico.rediris.es www.eldiario.es
;; ->>HEADER<<- opcode: QUERY, rcode: REFUSED, id: 60467
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; www.eldiario.es.     IN    A

;; ANSWER SECTION:

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 3 msec
;; SERVER: 130.206.1.3
;; WHEN: Wed Jan 15 13:10:59 2020
;; MSG SIZE  rcvd: 33
```

El siguiente ejemplo muestra una consulta que no se ha podido resolver por fallos en algún servidor de DNS:

```
$ drill www.undominio.es
;; ->>HEADER<<- opcode: QUERY, rcode: SERVFAIL, id: 34612
;; flags: qr rd ra ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; www.undominio.es.    IN    A

;; ANSWER SECTION:
```

```
;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 1282 msec
;; SERVER: 10.49.8.100
;; WHEN: Wed Jan 15 13:16:48 2020
;; MSG SIZE  rcvd: 34
```

El código de resultado SERVFAIL indica que algún problema en uno o varios de los servidores de DNS implicados ha impedido resolver la consulta. Por ejemplo, el servidor local no tenía la respuesta en su caché y cuando ha intentado buscarla recursivamente se ha encontrado con que en alguno de los pasos ningún servidor autoritativo le respondía o bien le rechazaba las consultas efectuadas.

El siguiente ejemplo muestra cómo se puede obtener un listado completo de una cierta zona:

```
$ drill -t @ns.etsist.upm.es axfr etsist.upm.es
```

La consulta se hace a un servidor autoritativo del dominio, se especifica el tipo de registro AXFR (que realmente no es un tipo de registro, sino una forma de indicar que se quiere el listado completo de la zona) y se especifica que se use TCP como protocolo de transporte, ya que con UDP la respuesta no suele caber en un solo datagrama.

Habitualmente las consultas como la anterior obtienen una respuesta de rechazo, pues los servidores autoritativos raramente permiten que cualquiera pueda obtener el listado completo de la zona.