Redes y Comunicaciones

DNS – Herramienta dig

Desafío – Herramienta cURL

DNS

Consultas recursivas

La consulta recursiva da una respuesta final sobre una consulta dada. Por ejemplo, ¿Cuál es la dirección de ada.info.unlp.edu.ar?

```
$ dig ada.info.unlp.edu.ar

; <<>> DiG 9.9.5-3ubuntu0.2-Ubuntu <<>> ada.info.unlp.edu.ar @200.49.130.44
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30777
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;ada.info.unlp.edu.ar.          IN      A

;; ANSWER SECTION:
ada.info.unlp.edu.ar.   86376   IN      A       163.10.5.66

;; Query time: 14 msec
;; SERVER: 200.49.130.44#53(200.49.130.44)
;; WHEN: Wed Mar 25 22:37:48 ART 2015
;; MSG SIZE  rcvd: 65
```

rd: (recursion desired) la consulta explícitamente solicita que se la maneje en forma recursiva.
ra: (recursion available) la consulta fue atendida en forma recursiva.
SERVER:(200.49.130.44): el servidor que respondió a la consulta fue el servidor 200.49.130.44

Consultas iterativas

Ante una consulta iterativa, un servidor ofrece la mejor respuesta que puede dar sin hacer consultas a otros servidores de DNS.
Por ejemplo, la consulta recursiva anterior que permitió asociar **ada.info.unlp.edu.ar** con la dirección **163.10.5.66**, pero ¿cómo hizo el servidor de DNS para saber la respuesta?

Fue con varias consultas iterativas

Internamente las consultas que hizo el servidor fueron:

1.- Determinar cuáles son los servidores de la zona "."

Estos están en un archivo de configuración en el servidor

```
# dig +norecurse -t ns .

;; ANSWER SECTION:
.                       304828 IN       NS      a.root-servers.net.
.                       304828 IN       NS      b.root-servers.net.
.                       304828 IN       NS      c.root-servers.net.
.                       304828 IN       NS      d.root-servers.net.
.                       304828 IN       NS      e.root-servers.net.
….

;; ADDITIONAL SECTION:
a.root-servers.net.     391222 IN       A       198.41.0.4
a.root-servers.net.     392652 IN       AAAA    2001:503:ba3e::2:30
b.root-servers.net.     391246 IN       A       192.228.79.201
b.root-servers.net.     486597 IN       AAAA    2001:500:84::b
c.root-servers.net.     391223 IN       A       192.33.4.12
c.root-servers.net.     392406 IN       AAAA    2001:500:2::c
d.root-servers.net.     601656 IN       A       199.7.91.13
….
```

2.- Preguntarle a alguno de los anteriores para que nos diga quién se encarga de la zona “AR”

 # dig +norecurse @192.33.4.12 -t ns ada.info.unlp.edu.ar

```
;; AUTHORITY SECTION:
ar.                     172800 IN       NS      relay1.mecon.gov.ar.
ar.                     172800 IN       NS      c.dns.ar.
ar.                     172800 IN       NS      ctina.ar.
ar.                     172800 IN       NS      ar.cctld.authdns.ripe.net.
ar.                     172800 IN       NS      ns2.switch.ch.
ar.                     172800 IN       NS      a.dns.ar.

;; ADDITIONAL SECTION:
a.dns.ar.               172800 IN       A       200.108.145.50
c.dns.ar.               172800 IN       A       200.108.148.50
ns2.switch.ch.          172800 IN       A       130.59.138.49
ctina.ar.               172800 IN       A       200.16.97.17
relay1.mecon.gov.ar.    172800 IN       A       168.101.16.10
```

3.- Preguntarle a alguno de los anteriores para que nos diga quien se encarga de la zona “EDU.AR”

 # dig +norecurse @200.16.97.17 -t ns ada.info.unlp.edu.ar

```
;; AUTHORITY SECTION:
edu.ar.                 86400   IN      NS      ns2.switch.ch.
edu.ar.                 86400   IN      NS      noc.uncu.edu.ar.
edu.ar.                 86400   IN      NS      ns1.uba.ar.
edu.ar.                 86400   IN      NS      ns1.riu.edu.ar.
edu.ar.                 86400   IN      NS      ns1.mrecic.gov.ar.
edu.ar.                 86400   IN      NS      ns2.mrecic.gov.ar.
edu.ar.                 86400   IN      NS      ns2.uba.ar.
edu.ar.                 86400   IN      NS      unlp.unlp.edu.ar.

;; ADDITIONAL SECTION:
noc.uncu.edu.ar.        86400   IN      A       170.210.2.97
ns1.riu.edu.ar.         86400   IN      A       170.210.0.18
ns1.uba.ar.             86400   IN      A       157.92.1.1
ns2.uba.ar.             86400   IN      A       157.92.4.1
unlp.unlp.edu.ar.       86400   IN      A       163.10.0.67
```

4.- Preguntarle a alguno de los anteriores para que nos diga quien se encarga de la zona “UNLP.EDU.AR”

$ dig +norecurse @157.92.1.1 -t ns ada.info.unlp.edu.ar

```
;; AUTHORITY SECTION:
unlp.edu.ar.            3600    IN      NS      unlp.unlp.edu.ar.
unlp.edu.ar.            3600    IN      NS      ns1.riu.edu.ar.
unlp.edu.ar.            3600    IN      NS      anubis.unlp.edu.ar.

;; ADDITIONAL SECTION:
ns1.riu.edu.ar.         3600    IN      A       170.210.0.18
unlp.unlp.edu.ar.       3600    IN      A       163.10.0.67
anubis.unlp.edu.ar.     3600    IN      A       163.10.0.65
```

5.- Preguntarle a alguno de los anteriores para que nos diga quien se encarga de la zona “INFO.UNLP.EDU.AR”

```
$ dig +norecurse @170.210.0.18 -t ns ada.info.unlp.edu.ar

;; AUTHORITY SECTION:
info.unlp.edu.ar.       86400   IN      NS      mail.linti.unlp.edu.ar.
info.unlp.edu.ar.       86400   IN      NS      anubis.unlp.edu.ar.
info.unlp.edu.ar.       86400   IN      NS      ada.info.unlp.edu.ar.

;; ADDITIONAL SECTION:
ada.info.unlp.edu.ar.   86400   IN      A       163.10.5.66
mail.linti.unlp.edu.ar. 86400   IN      A       163.10.10.61
anubis.unlp.edu.ar.     86400   IN      A       163.10.0.65
```

6.- Ahora que identificamos al servidor de la zona “INFO.UNLP.EDU.AR”, solo resta preguntarle quien es “ADA.INFO.UNLP.EDU.AR”

$ dig +norecurse @163.10.10.61 ada.info.unlp.edu.ar

```
;; ANSWER SECTION:
ada.info.unlp.edu.ar.    86400   IN      A       163.10.5.66

;; AUTHORITY SECTION:
info.unlp.edu.ar.        86400   IN      NS      mail.linti.unlp.edu.ar.
info.unlp.edu.ar.        86400   IN      NS      ada.info.unlp.edu.ar.
info.unlp.edu.ar.        86400   IN      NS      anubis.unlp.edu.ar.

;; ADDITIONAL SECTION:
mail.linti.unlp.edu.ar.  86400   IN      A       163.10.10.61
anubis.unlp.edu.ar.      46847   IN      A       163.10.0.65
```

DNS + SMTP

Si tengo una cuenta de email nico@info.unlp.edu.ar, y quiero mandarle un mail a un amigo cuyo mail es: tux@kernel.org. Al mandar el mail, mi servidor lo acepta, pero, ¿ cómo sabe a donde tiene que mandar ese correo para que le llegue a mi amigo?

Para responder poder responder esto, es necesario dar con el servidor de DNS que tiene bajo su administración el dominio “KERNEL.ORG”. Una vez identificado dicho servidor, al realizarle una consulta por los MX del dominio, me debería responder con las direcciones de los servidores de mail de dicho dominio.

Notar que estoy haciendo una consulta recursiva, por lo que el servidor que me la va a responder se va a encargar de contactar con los servidores del dominio deseado y darme la respuesta final a mi pregunta.

```
$ dig -t mx kernel.org
; <<>> DiG 9.9.5-3ubuntu0.2-Ubuntu <<>> -t mx kernel.org @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13939
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 3, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;kernel.org.                    IN      MX

;; ANSWER SECTION:
kernel.org.             600     IN      MX      999 bl-ckh-le.kernel.org.
kernel.org.             600     IN      MX      30 ns2.kernel.org.
kernel.org.             600     IN      MX      30 ns4.kernel.org.
kernel.org.             600     IN      MX      10 mail.kernel.org.

;; AUTHORITY SECTION:
kernel.org.             86399   IN      NS      ns4.kernel.org.
kernel.org.             86399   IN      NS      ns2.kernel.org.
kernel.org.             86399   IN      NS      ns0.kernel.org.

;; ADDITIONAL SECTION:
ns2.kernel.org.         86399   IN      A       149.20.4.80
ns2.kernel.org.         86399   IN      AAAA    2001:4f8:1:10::1:1
ns4.kernel.org.         86399   IN      A       199.204.44.194
ns0.kernel.org.         86399   IN      A       198.145.29.143

;; Query time: 1374 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Mar 25 22:49:07 ART 2015
;; MSG SIZE  rcvd: 248
```

Preguntas de comprensión

- Cuando mi amigo me responda, ¿Cuál es la dirección a la que su servidor de mails debería mandar la respuesta para que llegue a mi servidor?
- Si en mi cliente de correo tengo configurado mi servidor de correo electrónico usando su nombre (FQDN), por ej. **mx1.info.unlp.edu.ar**
    - Mi PC, ¿tiene que realizar una consulta de tipo A para contactarse con el servidor cuando yo mande un email?

Consultas Autoritativas y Consultas No Autoritativas

Dada la siguiente información:

```
$ host -t ns kernel.org
kernel.org name server ns0.kernel.org.
kernel.org name server ns4.kernel.org.
kernel.org name server ns2.kernel.org.
```

1. Analice la diferencia entre las siguientes consultas y determine que significa que una respuesta es AUTORITATIVA.
2. Indique cuál de las siguientes es AUTORITATIVA y cuál NO.

QUERY 1

```
$ dig @8.8.4.4 -t mx kernel.org
; <<>> DiG 9.9.5-3ubuntu0.2-Ubuntu <<>> @8.8.4.4 -t mx kernel.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65247
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;kernel.org.                    IN      MX

;; ANSWER SECTION:
kernel.org.             599     IN      MX      999 bl-ckh-le.kernel.org.
kernel.org.             599     IN      MX      10 mail.kernel.org.
kernel.org.             599     IN      MX      30 ns2.kernel.org.
kernel.org.             599     IN      MX      30 ns4.kernel.org.

;; Query time: 198 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Wed Mar 25 22:50:45 ART 2015
;; MSG SIZE  rcvd: 126
```

QUERY 2

```
$ dig @ns2.kernel.org -t mx kernel.org
; <<>> DiG 9.9.5-3ubuntu0.2-Ubuntu <<>> @ns2.kernel.org -t mx kernel.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46184
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 3, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;kernel.org.                    IN      MX

;; ANSWER SECTION:
kernel.org.             600     IN      MX      30 ns2.kernel.org.
kernel.org.             600     IN      MX      30 ns4.kernel.org.
kernel.org.             600     IN      MX      999 bl-ckh-le.kernel.org.
kernel.org.             600     IN      MX      10 mail.kernel.org.

;; AUTHORITY SECTION:
kernel.org.             86400   IN      NS      ns2.kernel.org.
kernel.org.             86400   IN      NS      ns0.kernel.org.
kernel.org.             86400   IN      NS      ns4.kernel.org.

;; ADDITIONAL SECTION:
mail.kernel.org.600     IN      A       198.145.29.136
ns2.kernel.org.         86400   IN      A       149.20.4.80
ns2.kernel.org.         86400   IN      AAAA    2001:4f8:1:10::1:1
ns4.kernel.org.         86400   IN      A       199.204.44.194
ns0.kernel.org.         86400   IN      A       198.145.29.143

;; Query time: 212 msec
;; SERVER: 149.20.4.80#53(149.20.4.80)
;; WHEN: Wed Mar 25 22:51:23 ART 2015
;; MSG SIZE  rcvd: 264
```

Desafío Capa de Aplicación

Para ejecutarlo deben:

1. Descargar el binario.
2. Abrir una terminal de root.
3. Darle permisos de ejecución al archivo: **chmod 755 binario**
4. Ejecutarlo con el parámetro correcto: **./binario <parámetro>**
5. Si esto pasa van a ver el mensaje: ******* El desafío está en marcha *****.**
6. Sino les va a indicar: **El parámetro ingresado es incorrecto. Volvé a intentarlo.**
7. Ahora les queda resolver el desafío…

Desafío Capa de Aplicación

Para averiguar el parámetro correcto se debe obtener el nombre de un servidor web.

¿Cómo podemos hacer esto?

¿Cómo encontramos esta información?

Desafío Capa de Aplicación

Hay varias formas de realizar esto. Una es directamente capturando con Wireshark un requerimiento web al servidor y buscando en los headers que responde el servidor la respuesta.

cURL

Otra forma de obtener la misma información es utilizando la herramienta **cURL**.

cURL es una herramienta que nos permite realizar distintas peticiones soportando diversos protocolos (DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPS, TELNET y TFTP) .

Veamos cómo funciona…

¿Pudieron resolver el desafío?