Redes de Ordenadores

GRADO EN INGENIERÍA INFORMÁTICA

Lr - DNS

Curso 2020/2021

Jorge Rodríguez Fraile, 100405951, Grupo 81, 100405951@alumnos.uc3m.es

Índice

Jorge Rodríguez Fraile, 100405951, Grupo 81

Cuestiones de nslookup

1. Ejecuta nslookup para obtener la dirección IP del dominio de la **Agencia Tributaria Española.**

   Su dirección IP de dominio es 195.77.198.25

```
C:\Users\Jorge>nslookup www.agenciatributaria.es
Server:  254.red-80-58-61.staticip.rima-tde.net
Address:  80.58.61.254

Non-authoritative answer:
Name:    www.agenciatributaria.es
Address:  195.77.198.25
```

2. Ejecuta nslookup para obtener los *authoritative servers* de **Yahoo**.

   Los servidores autoritarios para yahoo.com, con su nombre y dirección IP son:

   ns1.yahoo.com 68.180.131.16
   ns2.yahoo.com 68.142.255.16
   ns3.yahoo.com 27.123.42.42
   ns4.yahoo.com 98.138.11.157
   ns5.yahoo.com 202.165.97.53

```
C:\Users\Jorge>nslookup -type=NS yahoo.com
Server:  254.red-80-58-61.staticip.rima-tde.net
Address:  80.58.61.254

Non-authoritative answer:
yahoo.com       nameserver = ns2.yahoo.com
yahoo.com       nameserver = ns4.yahoo.com
yahoo.com       nameserver = ns3.yahoo.com
yahoo.com       nameserver = ns1.yahoo.com
yahoo.com       nameserver = ns5.yahoo.com

ns1.yahoo.com   AAAA IPv6 address = 2001:4998:130::1001
ns2.yahoo.com   AAAA IPv6 address = 2001:4998:140::1002
ns3.yahoo.com   AAAA IPv6 address = 2406:8600:f03f:1f8::1003
ns5.yahoo.com   AAAA IPv6 address = 2406:2000:ff60::53
ns1.yahoo.com   internet address = 68.180.131.16
ns2.yahoo.com   internet address = 68.142.255.16
ns3.yahoo.com   internet address = 27.123.42.42
ns4.yahoo.com   internet address = 98.138.11.157
ns5.yahoo.com   internet address = 202.165.97.53
```

3. Ejecuta nslookup para determinar los servidores de correo de la **Universidad Carlos III**

   Los servidores obtenidos del tipo MX, los de intercambio de correo, para uc3m.es son:

   aspmx.l.google.com internet address = 142.250.13.26
   aspmx.l.google.com AAAA IPv6 address = 2a00:1450:400c:c0c::1a
   alt1.aspmx.l.google.com internet address = 209.85.233.26
   alt1.aspmx.l.google.com AAAA IPv6 address = 2a00:1450:4010:c03::1a
   alt2.aspmx.l.google.com AAAA IPv6 address = 2404:6800:4003:c05::1a
   aspmx2.googlemail.com AAAA IPv6 address = 2a00:1450:4010:c03::1a
   aspmx3.googlemail.com internet address = 172.253.118.26
   aspmx3.googlemail.com AAAA IPv6 address = 2404:6800:4003:c05::1a

```
C:\Users\Jorge>nslookup -type=MX uc3m.es
Server:  254.red-80-58-61.staticip.rima-tde.net
Address:  80.58.61.254

Non-authoritative answer:
uc3m.es MX preference = 30, mail exchanger = aspmx3.googlemail.com
uc3m.es MX preference = 10, mail exchanger = aspmx.l.google.com
uc3m.es MX preference = 30, mail exchanger = aspmx2.googlemail.com
uc3m.es MX preference = 20, mail exchanger = alt2.aspmx.l.google.com
uc3m.es MX preference = 20, mail exchanger = alt1.aspmx.l.google.com

aspmx.l.google.com      internet address = 142.250.13.26
aspmx.l.google.com      AAAA IPv6 address = 2a00:1450:400c:c0c::1a
alt1.aspmx.l.google.com internet address = 209.85.233.26
alt1.aspmx.l.google.com AAAA IPv6 address = 2a00:1450:4010:c03::1a
alt2.aspmx.l.google.com AAAA IPv6 address = 2404:6800:4003:c05::1a
aspmx2.googlemail.com   AAAA IPv6 address = 2a00:1450:4010:c03::1a
aspmx3.googlemail.com   internet address = 172.253.118.26
aspmx3.googlemail.com   AAAA IPv6 address = 2404:6800:4003:c05::1a
```

Cuestiones escenario 1: Web-surfing

Source	Destination	Protocol	Length	Info
192.168.1.40	104.16.45.99	TCP	66	53805 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.40	80.58.61.254	DNS	91	Standard query 0x1bc9 A www.ietf.org.cdn.cloudflare.net
104.16.45.99	192.168.1.40	TCP	66	443 → 53805 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
192.168.1.40	104.16.45.99	TCP	54	53805 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
80.58.61.254	192.168.1.40	DNS	123	Standard query response 0x1bc9 A www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
192.168.1.40	104.16.45.99	TLSv1.3	571	Client Hello
104.16.45.99	192.168.1.40	TCP	60	443 → 53805 [ACK] Seq=1 Ack=518 Win=67584 Len=0
104.16.45.99	192.168.1.40	TLSv1.3	1506	Server Hello, Change Cipher Spec
104.16.45.99	192.168.1.40	TLSv1.3	1382	Application Data
192.168.1.40	104.16.45.99	TCP	54	53805 → 443 [ACK] Seq=518 Ack=2781 Win=263168 Len=0

4. Localiza los mensajes de petición y respuesta DNS. ¿Son enviados sobre TCP o sobre UDP?

Source	Destination	Protocol	Length	Info
192.168.1.40	80.58.61.254	DNS	91	Standard query 0x1bc9 A www.ietf.org.cdn.cloudflare.net
104.16.45.99	192.168.1.40	TCP	66	443 → 53805 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
192.168.1.40	104.16.45.99	TCP	54	53805 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
80.58.61.254	192.168.1.40	DNS	123	Standard query response 0x1bc9 A www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99

Son enviados con UDP.

```
User Datagram Protocol, Src Port: 49812, Dst Port: 53
```

5. ¿Cuál es el puerto de destino para el mensaje de petición DNS? ¿Cuál es el puerto de origen del mensaje respuesta?

Puerto destino de la petición: 53

Puesto origen de la respuesta: 53

```
User Datagram Protocol, Src Port: 49812, Dst Port: 53
```

```
User Datagram Protocol, Src Port: 53, Dst Port: 49812
```

6. ¿A qué dirección IP se envió la petición DNS? Utiliza alguna de las aplicaciones del sistema comentadas anteriormente para determinar la dirección IP del servidor DNS configurado en el equipo. ¿Coinciden ambas direcciones?

La petición se envió a la dirección: 80.58.61.254

Wireshark:

Source	Destination	Protocol	Length	Info
192.168.1.40	80.58.61.254	DNS	91	Standard query 0x1bc9 A www.ietf.org.cdn.cloudflare.net

nslookup:

```
C:\Users\Jorge>nslookup
Default Server:  254.red-80-58-61.staticip.rima-tde.net
Address:  80.58.61.254
```

Ambas coinciden.

7. Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene el mensaje de petición alguna respuesta (answer)?

Es de tipo A, dado el nombre del servidor obtenemos su dirección IP. No contienen ninguna respuesta la petición.

```
Queries
  www.ietf.org.cdn.cloudflare.net: type A, class IN
      Name: www.ietf.org.cdn.cloudflare.net
      [Name Length: 31]
      [Label Count: 6]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

```
Domain Name System (query)
  Transaction ID: 0x1bc9
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
```

8. Examina el mensaje de respuesta DNS. ¿Cuántas respuestas contiene? ¿Qué contiene cada una de esas respuestas?

   Contiene 2 respuestas, ambas sobre el mismo servidor, que nos proporcionan las IP que podemos utilizar para comunicarnos, 104.16.45.99 y 104.16.44.99.

```
Domain Name System (response)
    Transaction ID: 0x1bc9
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Answers
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
          Name: www.ietf.org.cdn.cloudflare.net
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 300 (5 minutes)
          Data length: 4
          Address: 104.16.45.99
    v www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
          Name: www.ietf.org.cdn.cloudflare.net
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 300 (5 minutes)
          Data length: 4
          Address: 104.16.44.99
```

9. Considera el siguiente paquete TCP SYN enviado por tu host. ¿Se corresponde la IP de destino a alguna de las direcciones IP contenidas en el mensaje de respuesta DNS?

   El mensaje de SYN lo envía a la dirección 104.16.45.99, que era una de las respuestas a la petición.

Source	Destination	Protocol	Length	Info
192.168.1.40	104.16.45.99	TCP	66	53805 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

10. Esta página web contiene imágenes. ¿Antes de descargar cada imagen se realizan nuevas peticiones DNS?

    No, no se hace ninguna petición DNS más en el periodo capturado.

Cuestiones escenario 2: nslookup

11. ¿Cuál es el puerto destino para el mensaje de petición DNS? ¿Cuál es el puerto origen del mensaje respuesta DNS?

    Puerto destino de la petición: 53

    Puesto origen de la respuesta: 53

```
User Datagram Protocol, Src Port: 60017, Dst Port: 53
```

```
User Datagram Protocol, Src Port: 53, Dst Port: 60017
```

12. ¿A qué dirección IP se envía el mensaje de petición DNS? ¿Se corresponde esa IP con la configurada en el equipo para el servidor DNS por defecto?

    La petición se envía a 80.58.61.254, que se corresponde con la por defecto del sistema.

```
192.168.1.40        80.58.61.254        DNS        71 Standard query 0x0002 A www.uc3m.es
```

```
C:\Users\Jorge>nslookup
Default Server:  254.red-80-58-61.staticip.rima-tde.net
Address:  80.58.61.254
```

13. Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene dicho mensaje alguna respuesta (answer)?

    El registro es de tipo A, correspondencia nombre e IP.

```
Queries
  www.uc3m.es: type A, class IN
      Name: www.uc3m.es
      [Name Length: 11]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

    No contiene ninguna respuesta la petición.

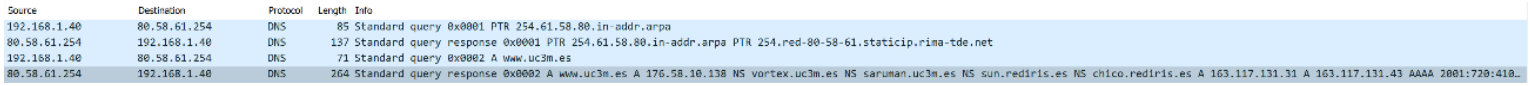
```
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

14. Examina el mensaje de respuesta DNS. ¿Cuántas respuestas contiene? ¿Qué contiene cada una de esas respuestas?

    Contiene 1 respuesta, la dirección IP del nombre www.uc3m.es, y además contiene 4 nombres de servidores de nombres y las direcciones IPv4 y IPv6 de dos de ellos.

```
Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 4
Answers
  > www.uc3m.es: type A, class IN, addr 176.58.10.138
Authoritative nameservers
  > uc3m.es: type NS, class IN, ns vortex.uc3m.es
  > uc3m.es: type NS, class IN, ns saruman.uc3m.es
  > uc3m.es: type NS, class IN, ns sun.rediris.es
  > uc3m.es: type NS, class IN, ns chico.rediris.es
Additional records
  > vortex.uc3m.es: type A, class IN, addr 163.117.131.31
  > saruman.uc3m.es: type A, class IN, addr 163.117.131.43
  > vortex.uc3m.es: type AAAA, class IN, addr 2001:720:410:b131::31
  > saruman.uc3m.es: type AAAA, class IN, addr 2001:720:410:b131::43
```

15. Adjunta una captura de pantalla



Source	Destination	Protocol	Length	Info
192.168.1.40	80.58.61.254	DNS	85	Standard query 0x0001 PTR 254.61.58.80.in-addr.arpa
80.58.61.254	192.168.1.40	DNS	137	Standard query response 0x0001 PTR 254.61.58.80.in-addr.arpa PTR 254.red-80-58-61.staticip.rima-tde.net
192.168.1.40	80.58.61.254	DNS	71	Standard query 0x0002 A www.uc3m.es
80.58.61.254	192.168.1.40	DNS	264	Standard query response 0x0002 A www.uc3m.es A 176.58.10.138 NS vortex.uc3m.es NS saruman.uc3m.es NS sun.rediris.es NS chico.rediris.es A 163.117.131.31 A 163.117.131.43 AAAA 2001:720:410…

Jorge Rodríguez Fraile, 100405951, Grupo 81

Cuestiones escenario 3: nslookup

16. ¿A qué dirección IP se envía el mensaje de petición DNS? ¿Se corresponde esa IP con la configurada en el equipo para el servidor DNS por defecto?

    Se envía a la dirección 80.58.61.254. Se corresponde con la IP configurada en el equipo por defecto.

```
192.168.1.40        80.58.61.254        DNS        67 Standard query 0x0002 NS uc3m.es
```

```
Address:  80.58.61.254
```

17. Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene dicho mensaje alguna respuesta (answer)?

    El registro es de tipo NS, que proporcionan la correspondencia del nombre de dominio con los servidores de nombres.

    No contiene ninguna respuesta la petición.

```
Queries
  uc3m.es: type NS, class IN
      Name: uc3m.es
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
```

```
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

18. Examina el mensaje de respuesta DNS. ¿Qué servidores de nombres aparecen en el mensaje de respuesta para la Universidad Carlos III? ¿Proporciona esta respuesta las direcciones IP de dichos servidores?

    Servidores de nombres: vorteX.uc3m.es, saruman.uc3m.es, sun.rediris.es, chico.rediris.es

```
  Answers
    > uc3m.es: type NS, class IN, ns chico.rediris.es
    > uc3m.es: type NS, class IN, ns saruman.uc3m.es
    > uc3m.es: type NS, class IN, ns vortex.uc3m.es
    > uc3m.es: type NS, class IN, ns sun.rediris.es
```

    Proporciona las direcciones IPv4 y IPv6 de dos de ellos:

    sun.rediris.es: 199.184.182.1 y 2620:171:808::1

    chico.rediris.es: 162.219.54.2 y 2620:10a:80eb::2

```
Additional records
  > sun.rediris.es: type A, class IN, addr 199.184.182.1
  > sun.rediris.es: type AAAA, class IN, addr 2620:171:808::1
  > chico.rediris.es: type A, class IN, addr 162.219.54.2
  > chico.rediris.es: type AAAA, class IN, addr 2620:10a:80eb::2
```

19. Adjunta una captura de pantalla

```
192.168.1.40        80.58.61.254        DNS        67 Standard query 0x0002 NS uc3m.es
80.58.61.254        192.168.1.40        DNS       244 Standard query response 0x0002 NS uc3m.es NS chico.rediris.es NS saruman.uc3m.es NS vortex.uc3m.es NS sun.rediris.es A 199.184.182.1 AAAA 2620:171:808::1 A 162.219.54.2 AAAA 2620:10a:80eb…
```

Jorge Rodríguez Fraile, 100405951, Grupo 81

Cuestiones escenario 4: nslookup

20. ¿A qué dirección IP se envía el mensaje de petición DNS? ¿Se corresponde esa IP con la configurada en el equipo para el servidor DNS por defecto? Si no lo es, ¿a qué dirección IP se corresponde?

    La petición se envía a 163.117.131.31. No se trata de la que tiene por defecto el sistema, , ya que lo hemos especificado en el comando. La IP se corresponde al servidor de nombres, vortex.uc3m.es, con IP 163.117.131.31 que la hemos tenido que solicitar.

```
192.168.1.40          163.117.131.31        DNS          71 Standard query 0x0002 A www.uc3m.es
Address:  80.58.61.254                      Standard query response 0xb278 A vortex.uc3m.es A 163.117.131.31
```

21. Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene dicho mensaje alguna respuesta (answer)?

    El registro es de tipo A, queremos la IP ligada al nombre www.uc3m.es. No contienen ninguna respuesta.

```
Queries                                  Domain Name System (query)
  www.uc3m.es: type A, class IN            Transaction ID: 0x0002
      Name: www.uc3m.es                  > Flags: 0x0100 Standard query
      [Name Length: 11]                    Questions: 1
      [Label Count: 3]                     Answer RRs: 0
      Type: A (Host Address) (1)           Authority RRs: 0
      Class: IN (0x0001)                   Additional RRs: 0
```

22. Examina el mensaje de respuesta DNS. ¿Cuántas respuestas contiene? ¿Qué contiene cada una de esas respuestas?

    Contiene una sola respuesta, la dirección IP del nombre de dominio solicitado, 176.58.10.138. Aunque también incluye los servidores de nombre y algunas de sus direcciones IP.

```
Domain Name System (response)
   Transaction ID: 0x0002
 > Flags: 0x8500 Standard query response, No error
   Questions: 1
   Answer RRs: 1
   Authority RRs: 4
   Additional RRs: 4

Answers
 > www.uc3m.es: type A, class IN, addr 176.58.10.138
Authoritative nameservers
 > uc3m.es: type NS, class IN, ns saruman.uc3m.es
 > uc3m.es: type NS, class IN, ns vorteX.uc3m.es
 > uc3m.es: type NS, class IN, ns chico.rediris.es
 > uc3m.es: type NS, class IN, ns sun.rediris.es
Additional records
 > vorteX.uc3m.es: type A, class IN, addr 163.117.131.31
 > saruman.uc3m.es: type A, class IN, addr 163.117.131.43
 > vorteX.uc3m.es: type AAAA, class IN, addr 2001:720:410:b131::31
 > saruman.uc3m.es: type AAAA, class IN, addr 2001:720:410:b131::43
```

23. Adjunta una captura de pantalla

```
192.168.1.40      80.58.61.254      DNS       74 Standard query 0xb278 A vortex.uc3m.es
80.58.61.254      192.168.1.40      DNS      244 Standard query response 0xb278 A vortex.uc3m.es A 163.117.131.31 NS saruman.uc3m.es NS vortex.uc3m.es NS chico.rediris.es NS sun.rediris.es A 163.117.131.43 AAAA 2001:720:410:b131::31 AAA…
192.168.1.40      163.117.131.31    DNS       87 Standard query 0x0001 PTR 31.131.117.163.in-addr.arpa
163.117.131.31    192.168.1.40      DNS      285 Standard query response 0x0001 PTR 31.131.117.163.in-addr.arpa PTR vorteX.uc3m.es NS sun.rediris.es NS vorteX.uc3m.es NS chico.rediris.es NS saruman.uc3m.es A 163.117.131.31 A 163.117.131…
192.168.1.40      163.117.131.31    DNS       71 Standard query 0x0002 A www.uc3m.es
163.117.131.31    192.168.1.40      DNS      264 Standard query response 0x0002 A www.uc3m.es A 176.58.10.138 NS saruman.uc3m.es NS vorteX.uc3m.es NS chico.rediris.es NS sun.rediris.es A 163.117.131.31 A 163.117.131.43 AAAA 2001:720:410…
```