

# Fundamentos de Redes de Datos

## Tarea 2: Arquitectura de Red

Utiliza el programa *Wireshark* para capturar el tráfico de red en el interfaz principal de un computador cualquiera (puedes hacerlo en un laboratorio, tu portátil, tu PC de casa, o cualquier otro en el que esté instalado dicho programa). Asegúrate de que, durante el periodo de captura, se captura al menos tráfico correspondiente a una consulta DNS, así como una petición de una página web a un servidor cualquiera.

1. Especifica los comandos / programas utilizados durante la captura para asegurarte de que se generaban tramas con los dos tipos de tráfico (DNS y HTTP) solicitados.

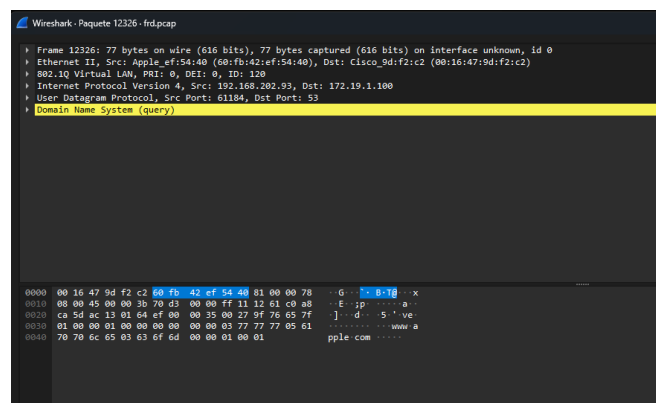
|             |                                  |           |  |
|-------------|----------------------------------|-----------|--|
| 0.000000    | HostsTechno.es:8122... Broadcast | ARP       | 42 who has 192.168.18.252? Tell 192.168.18.1                             |
| 0.000000    | 192.168.18.1                     | TCP       | 64431 → 443 [RST] Seq=1000000000 Win=0 Len=0                             |
| 3.1.286350  | 192.168.18.198                   | DNS       | 92 Standard query 0x657f A www.apple.com                                 |
| 4.1.286340  | 192.168.18.1                     | DNS       | 214 Standard query response 0x657f A www.apple.com                       |
| 5.1.286340  | 192.168.18.198                   | TCP       | 70 60831 → 443 [SYN] Seq=1000000000 Win=0 Len=0                          |
| 6.1.556092  | 20.189.173.21                    | TCP       | 74 443 → 49831 [SYN, ACK] Seq=1000000000 Win=5535 Len=0                  |
| 7.1.556257  | 192.168.18.198                   | TCP       | 66 49831 → 443 [ACK] Seq=1000000000 Win=0 Len=0                          |
| 8.1.558997  | 192.168.18.198                   | TLSv1.2   | 281 Client Hello   |
| 9.1.531568  | 13.107.42.12                     | TCP       | 54 443 → 49716 [RST, ACK] Seq=1000000000 Win=0 Len=0                     |
| 10.1.675873 | 20.189.173.21                    | TCP       | 1466 443 → 49831 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 11.1.691898 | 20.189.173.21                    | TCP       | 1466 443 → 49831 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 12.1.691930 | 192.168.18.198                   | TCP       | 66 49831 → 443 [ACK] Seq=1000000000 Win=0 Len=0                          |
| 13.1.643803 | 2280.10.104.0/24                 | Broadcast | 42 who has 192.168.18.45? Tell 192.168.18.1                              |
| 14.1.945443 | 20.189.173.21                    | TCP       | 1466 443 → 49831 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 15.1.945462 | 20.189.173.21                    | TLSv1.2   | 383 Server Hello, Certificate, Server Key Exchange, Server Hello Done    |
| 16.1.945718 | 192.168.18.198                   | TCP       | 66 49831 → 443 [ACK] Seq=1000000000 Win=0 Len=0                          |
| 17.1.959177 | 192.168.18.198                   | TLSv1.2   | 224 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 18.1.150426 | 20.189.173.21                    | TLSv1.2   | 117 Change Cipher Spec, Encrypted Handshake Message                      |
| 19.1.170559 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 20.1.170899 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 21.2.163172 | 20.189.173.21                    | TCP       | 66 443 → 49831 [ACK] Seq=1000000000 Win=1400 Len=0                       |
| 22.2.163445 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 23.2.163445 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 24.2.163445 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 25.2.170640 | 20.189.173.21                    | TCP       | 66 443 → 49831 [ACK] Seq=1000000000 Win=1400 Len=0                       |
| 26.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 27.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 28.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 29.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 30.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 31.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 32.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 33.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 34.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 35.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 36.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 37.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 38.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 39.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |
| 40.2.170720 | 192.168.18.198                   | TCP       | 1466 49831 → 443 [ACK] Seq=1000000000 Win=1400 Len=0                     |

En la barra de búsqueda de Wireshark puedo determinar el tipo de protocolo que quiero a modo de filtrado.

| No.   | Time      | Source         | Destination   | Protoc | Leng | Info                                     |
|-------|-----------|----------------|---------------|--------|------|--|
| 12... | 6.800000  | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x657f A www.apple.com    |
| 12... | 6.800000  | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x0dde AAAA www.apple.com |
| 13... | 7.800000  | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x657f A www.apple.com    |
| 13... | 7.800000  | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x0dde AAAA www.apple.com |
| 18... | 10.800000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x9fe3 A www.apple.com    |
| 18... | 10.800000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x8b0f AAAA www.apple.com |
| 34... | 19.820000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x9fe3 A www.apple.com    |
| 34... | 19.820000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x8b0f AAAA www.apple.com |
| 41... | 24.010000 | 192.168.202.97 | 156.154.70.22 | DNS    | 78   | Standard query 0xe415 A www.comodo.com   |
| 43... | 25.010000 | 192.168.202.97 | 8.26.56.26    | DNS    | 78   | Standard query 0xe415 A www.comodo.com   |
| 45... | 26.030000 | 192.168.202.97 | 156.154.70.22 | DNS    | 78   | Standard query 0xe415 A www.comodo.com   |
| 49... | 28.040000 | 192.168.202.97 | 8.26.56.26    | DNS    | 78   | Standard query 0xe415 A www.comodo.com   |
| 49... | 28.040000 | 192.168.202.97 | 156.154.70.22 | DNS    | 78   | Standard query 0xe415 A www.comodo.com   |
| 56... | 32.050000 | 192.168.202.97 | 8.26.56.26    | DNS    | 78   | Standard query 0xe415 A www.comodo.com   |
| 56... | 32.050000 | 192.168.202.97 | 156.154.70.22 | DNS    | 78   | Standard query 0xe415 A www.comodo.com   |
| 64... | 36.860000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x5a80 A www.apple.com    |
| 64... | 36.860000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x7970 AAAA www.apple.com |
| 66... | 37.860000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x5a80 A www.apple.com    |
| 66... | 37.860000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x7970 AAAA www.apple.com |
| 72... | 40.870000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x3f81 A www.apple.com    |
| 72... | 40.870000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x844d AAAA www.apple.com |
| 87... | 49.890000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x3f81 A www.apple.com    |
| 87... | 49.890000 | 192.168.202.93 | 172.19.1.100  | DNS    | 77   | Standard query 0x844d AAAA www.apple.com |

| No. | Time     | Source          | Destination     | Protocol | Length | Info                         |
|-----|----------|-----------------|-----------------|----------|--------|------------------------------|
| 40  | 0.000000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 236    | HEAD /DEASLog02.nsf HTTP/1.1 |
| 50  | 0.010000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 52  | 0.020000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 236    | HEAD /DEASLog03.nsf HTTP/1.1 |
| 77  | 0.030000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 87  | 0.030000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 236    | HEAD /DEASLog04.nsf HTTP/1.1 |
| 110 | 0.040000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 119 | 0.040000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 236    | HEAD /DEASLog05.nsf HTTP/1.1 |
| 143 | 0.050000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 151 | 0.060000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 234    | HEAD /decsadm.nsf HTTP/1.1   |
| 187 | 0.070000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 189 | 0.070000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 234    | HEAD /decslog.nsf HTTP/1.1   |
| 214 | 0.080000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 223 | 0.080000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 236    | HEAD /DEESAdmin.nsf HTTP/1.1 |
| 247 | 0.090000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 256 | 0.100000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 235    | HEAD /doladmin.nsf HTTP/1.1  |
| 287 | 0.110000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 289 | 0.110000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 235    | HEAD /domadmin.nsf HTTP/1.1  |
| 316 | 0.120000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 322 | 0.120000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 235    | HEAD /domguide.nsf HTTP/1.1  |
| 354 | 0.130000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 357 | 0.140000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 233    | HEAD /domlog.nsf HTTP/1.1    |
| 380 | 0.150000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 390 | 0.150000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 235    | HEAD /domguide.nsf HTTP/1.1  |
| 418 | 0.160000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 284    | HTTP/1.1 404 Not Found       |
| 424 | 0.160000 | 192.168.229.251 | 192.168.202.79  | HTTP     | 233    | HEAD /domlog.nsf HTTP/1.1    |
| 447 | 0.170000 | 192.168.202.79  | 192.168.229.251 | HTTP     | 233    | HEAD /domlog.nsf HTTP/1.1    |

2. Escoge una cualquiera de las tramas DNS capturadas y, adjuntando un pantallazo de ésta en el que aparezca claramente toda la información necesaria, contesta a los siguientes apartados:



- a) ¿Qué protocolo de transporte encapsula al mensaje original DNS de la capa de aplicación? Especifica cuál es el tamaño exacto (en bytes) del mensaje a nivel de aplicación, así como el de la cabecera añadida por dicho protocolo.

El protocolo de transporte que encapsula el mensaje DNS es normalmente **UDP**. El tamaño exacto del mensaje DNS es de **77 bytes** y la cabecera UDP tiene un tamaño fijo de **8 bytes**.

- b) ¿Dentro de qué protocolo de red viaja el anterior segmento? ¿Cuál es el tamaño en bytes añadido por la cabecera de este otro protocolo?

El segmento viaja dentro de la **IPv4**, con una cabecera de **20 bytes**.

- c) ¿Cuál es el tamaño total de la trama Ethernet que encapsula al segmento anterior?

El tamaño total de la trama Ethernet es de **77 bytes**, donde se incluye la cabecera Ethernet (14 bytes), la cabecera IP (20 bytes), la cabecera UDP (8 bytes) y los datos del mensaje DNS.

- d) Calcula la eficiencia de uso en % (es decir, el porcentaje de datos del nivel de aplicación enviados respecto al tamaño total final de la trama, que incluye todas las cabeceras de protocolos encapsulados comentados).

Para calcular la eficiencia de uso (%), utilizaremos la siguiente fórmula:

$$\text{Eficiencia} = \left( \frac{\text{Tamaño de los datos a nivel de aplicación}}{\text{Tamaño total de la trama}} \right) \times 100$$

- Datos a nivel de aplicación (DNS): 77 bytes
- Ethernet: 14 bytes
- IP: 20 bytes
- UDP: 8 bytes

$$\text{Eficiencia} = \left( \frac{77 - (14 + 20 + 8)}{77} \right) \times 100 = \left( \frac{35}{77} \right) \times 100 \approx 45.45\%$$

3. Repite el ejercicio anterior, con todos sus subapartados, pero en este caso para una trama cualquiera correspondiente al tráfico HTTP generado durante la captura.

```

Wireshark · Paquete 17 · frd.pcap
▶ Frame 17: 236 bytes on wire (1888 bits), 236 bytes captured (1888 bits) on interface unknown, id 0
▶ Ethernet II, Src: VMware_41:4b:e7 (00:0c:29:41:4b:e7), Dst: Cisco_9d:f2:c2 (00:16:47:9d:f2:c2)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 120
▶ Internet Protocol Version 4, Src: 192.168.202.79, Dst: 192.168.229.251
▶ Transmission Control Protocol, Src Port: 50465, Dst Port: 80, Seq: 1, Ack: 1, Len: 166
▶ Hypertext Transfer Protocol

0000  00 16 47 9d f2 c2 00 0c 29 41 4b e7 81 00 00 78  ..G....)AK...x
0010  08 00 45 00 00 da 7e 25 40 00 40 06 8a 5c c0 a8  ..E....% @.@\..
0020  ca 4f c0 a8 e5 fb c5 21 00 50 9e b2 07 e5 b5 8e  ..O....! .P.....
0030  17 93 80 18 03 91 15 bc 00 00 01 01 08 0a 00 86  ..y....HE AD /DEAS
0040  79 c7 00 00 00 00 48 45 41 44 20 2f 44 45 41 53  Log02.ns f HTTP/1
0050  4c 6f 67 30 32 2e 6e 73 66 20 48 54 54 50 2f 31  .1..Conn ection:
0060  2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20  close..U ser-Agen
0070  63 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65 6e  t: Mozil la/5.0 (
0080  74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28  compatib le; Nmap
0090  63 6f 6d 70 61 74 69 62 6c 65 3b 20 4e 6d 61 70  Scripti ng Engin
00a0  20 53 63 72 69 70 74 69 6e 67 20 45 6e 67 69 6e  e; http: //nmap.o
00b0  65 3b 20 68 74 74 70 3a 2f 2f 6e 6d 61 70 2e 6f  rg/book/ nse.html
00c0  72 67 2f 62 6f 6f 6b 2f 6e 73 65 2e 68 74 6d 6c  )..Host: 192.168
00d0  29 0d 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38  .229.251 ....
00e0  2e 32 32 39 2e 32 35 31 0d 0a 0d 0a
  
```

- a) El tráfico HTTP viaja encapsulado en **TCP**. En la captura se observa que el tamaño del mensaje es de **166 bytes**, pero la cabecera TCP tiene **20 bytes** (sin opciones adicionales).

- b) El segmento viaja dentro de la **IP**, con una cabecera de **20 bytes**.
- c) El tamaño total de la trama es de **236 bytes**. Este valor incluye la cabecera Ethernet (14 bytes), la cabecera IP, la cabecera TCP y los datos HTTP.
- d) Para calcular la eficiencia de uso (%), utilizaremos la siguiente fórmula:

$$\text{Eficiencia} = \left( \frac{\text{Tamaño de los datos a nivel de aplicación}}{\text{Tamaño total de la trama}} \right) \times 100$$

- Datos a nivel de aplicación (DNS): 166 bytes
- Ethernet: 14 bytes
- IP: 20 bytes
- TCP: 20 bytes

$$\text{Eficiencia} = \left( \frac{166}{236} \right) \times 100 \approx 70.34\%$$

4. En función de los resultados que obtengas en las preguntas anteriores, ¿podrías afirmar cuál de los dos casos es más eficiente desde el punto de vista del porcentaje de datos útiles enviados?

La trama HTTP es más eficiente desde el punto de vista del porcentaje de datos útiles enviados. Esto se debe a que, en el caso del tráfico HTTP, la proporción de datos de aplicación respecto al tamaño total de la trama es mayor, lo que implica un menor porcentaje de bytes destinados a las cabeceras.

5. Dada una arquitectura de red, reflexiona brevemente sobre las implicaciones derivadas de tener un número determinado de capas. Por ejemplo, ¿crees que a mayor número de capas siempre habrá un mayor número de bytes de cabecera?

Un mayor número de capas tiende a aumentar la cantidad de bytes de cabecera, pero este es un **compromiso necesario** para garantizar la **funcionalidad**, **modularidad**, y **escalabilidad** de la red. Aunque este incremento en la sobrecarga puede reducir la eficiencia de transmisión en términos de bytes útiles, aporta beneficios importantes en términos de flexibilidad, facilidad de mantenimiento, y capacidad para adaptarse a diferentes entornos de red.

6. Finalmente, ¿crees que un router necesita acceder a los datos a nivel aplicación (por ejemplo a los mensajes HTTP) para hacer su trabajo? ¿Podrías citar algún tipo de analogía similar relacionada con el transporte de información (no necesariamente en Internet) para reafirmar tu respuesta?

No, un router no necesita acceder a los datos del nivel de aplicación, como los mensajes HTTP, para hacer su trabajo. El router solo necesita información contenida en la cabecera de la capa de red (principalmente la dirección IP de destino), junto con algunas otras informaciones de control, para determinar el mejor camino para el paquete a través de la red.

Una analogía adecuada para entender esto sería:

- Imagina que tienes un **servicio postal**. Supongamos que deseas enviar una carta desde una ciudad a otra.
- El **cartero o sistema postal** (el equivalente al router) solo necesita ver la **dirección** escrita en el sobre (similar a la dirección IP en la cabecera de la capa de red). El cartero no necesita abrir la carta para ver su contenido (equivalente a los datos de la aplicación como HTTP).
- El contenido de la carta es irrelevante para el cartero porque su trabajo es únicamente entregar el sobre al destinatario correcto basándose en la dirección.

De forma similar, el router se centra únicamente en la información de direccionamiento de los paquetes, sin preocuparse por el contenido de los mismos, lo cual está en capas más altas (como la capa de aplicación).