Trabajo práctico N° 8 - Análisis de tramas

Santiago Fonzo

Instituto Superior Zona Oeste

Redes y comunicación

Ing. Ricardo Brisighelli

30 de enero de 2025

Objetivos

- Comprender el modelo OSI
- Analizar las funciones de la capa de red
- Identificar las tramas ethernet que circulan por una red
- Analizar las cabeceras de los protocolos involucrados
- Comprender el encapsulamiento de protocolos

Consignas a resolver

1. Analizar las siguientes tramas y sus datagramas

Trama A:

```
00 1d 72 62 a2 bb 00 19 db 7c dd 0f 08 00 45 10
01 48 00 00 00 00 80 11 d2 d2 be 1f e5 ee c0 a8
02 0c 00 43 00 44 01 34 db 4c 02 01 06 00 a0 54
13 3e 00 00 00 00 00 00 00 00 c0 a8 02 0c 00 00
00 00 00 00 00 00 00 1d 72 62 a2 bb 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 63 82 53 63 35 01 02 36 04 be
1f e5 ee 33 04 00 00 a8 c0 01 04 ff ff ff 00 00
04 c0 a8 02 01 0f 06 65 73 74 69 6c 6f 06 04 c0
a8 02 01 2a 04 c0 a8 02 01 ff 00 00 00 00 00
00 00 00 00 00 00
```

Trama B:

```
00 19 db 7c dd 0f 00 1d 72 62 a2 bb 08 00 45 00
03 a1 17 1b 40 00 40 06 c8 c9 c0 a8 02 0c d1 55
c3 68 cf af 00 50 94 30 a0 01 20 15 1b e4 80 18
00 2e c1 20 00 00 01 01 08 0a 00 05 b7 1b d9 de
1b f9 47 45 54 20 2f 66 69 72 65 66 6f 78 3f 63
6c 69 65 6e 74 3d 66 69 72 65 66 6f 78 2d 61 26
```

```
72 6c 73 3d 6f 72 67 2e 67 65 6e 74 6f 6f 3a 65
6e 2d 55 53 3a 6f 66 66 69 63 69 61 6c 20 48 54
54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 65 6e
2d 75 73 2e 73 74 61 72 74 33 2e 6d 6f 7a 69 6c
6c 61 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65
6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20
28 58 31 31 3b 20 55 3b 20 4c 69 6e 75 78 20 78
38 36 5f 36 34 3b 20 65 6e 2d 55 53 3b 20 72 76
3a 31 2e 39 2e 32 2e 33 29 20 47 65 63 6b 6f 2f
32 30 31 30 30 34 32 32 20 47 65 6e 74 6f 6f 20
46 69 72 65 66 6f 78 2f 33 2e 36 2e 33 20 47 54
42 37 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65
78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74
69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70
70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d
30 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41
63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20
65 73 2d 65 73 2c 65 73 3b 71 3d 30 2e 38 2c 65
6e 2d 75 73 3b 71 3d 30 2e 35 2c 65 6e 3b 71 3d
30 2e 33 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f
64 69 6e 67 3a 20 67 7a 69 70 2c 64 65 66 6c 61
74 65 0d 0a 41 63 63 65 70 74 2d 43 68 61 72 73
65 74 3a 20 49 53 4f 2d 38 38 35 39 2d 31 2c 75
74 66 2d 38 3b 71 3d 30 2e 37 2c 2a 3b 71 3d 30
2e 37 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a 20
31 31 35 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a
20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6f
6b 69 65 3a 20 5f 5f 75 74 6d 61 3d 31 38 33 38
35 39 36 34 32 2e 31 38 30 36 36 31 35 31 31 38
2e 31 32 33 39 32 37 37 35 30 38 2e 31 32 36 36
34 31 32 31 39 33 2e 31 32 36 38 30 34 39 36 30
39 2e 31 37 3b 20 73 5f 76 69 3d 5b 43 53 5d 76
31 7c 34 39 44 44 45 30 32 35 30 30 30 30 32 30
30 32 2d 41 30 32 30 38 30 35 30 30 30 30 30 30
39 34 5b 43 45 5d 3b 20 5f 5f 75 74 6d 7a 3d 31
38 33 38 35 39 36 34 32 2e 31 32 36 35 38 34 30
39 35 38 2e 31 35 2e 32 2e 75 74 6d 63 63 6e 3d
28 72 65 66 65 72 72 61 6c 29 7c 75 74 6d 63 73
72 3d 73 75 70 70 6f 72 74 2e 6d 6f 7a 69 6c 6c
61 2e 63 6f 6d 7c 75 74 6d 63 63 74 3d 2f 65 73
2f 6b 62 2f 46 69 72 65 66 6f 78 2b 48 65 6c 70
7c 75 74 6d 63 6d 64 3d 72 65 66 65 72 72 61 6c
3b 20 73 5f 76 73 6e 5f 6d 6f 7a 69 6c 6c 61 63
6f 6d 5f 31 3d 34 36 38 35 30 38 33 37 37 37 35
```

```
31 36 3b 20 53 53 49 44 5f 53 55 4d 4f 3d 69 62
42 37 53 55 30 34 6f 56 31 77 30 4c 69 4f 70 52
30 64 3b 20 57 54 5f 46 50 43 3d 69 64 3d 32 66
63 33 65 35 65 63 63 35 31 35 38 66 35 32 66 34
63 31 32 37 32 30 39 37 31 37 38 39 38 30 3a 6c
76 3d 31 32 37 32 30 39 37 31 37 38 39 38 30 3a
73 73 3d 31 32 37 32 30 39 37 31 37 38 39 38 30
3b 20 53 53 49 44 3d 69 62 53 5a 66 76 30 51 65
53 32 79 30 54 63 77 54 50 30 76 0d 0a 0d 0a
```

1. Análisis de trama y datagrama A

Dado que los bytes proporcionados no incluyen el preámbulo (aa aa aa aa aa aa aa) ni el byte de inicio de trama (ab), se considera que los datos comienzan desde la dirección física (MAC) de destino.

Cuando se considera necesario es adopta la nomenclatura siguiente:

Campo: (nibble/s correspondientes en hex) → Interpretación o equivalente binario

Cabecera Ethernet

- Dirección física de destino: 00:1d:72:62:a2:bb.
- Dirección física de origen: 00:19:db:7c:dd:0f.
- Tipo de protocolo del datagrama encapsulado: (08 00) → Protocolo IP. Los 4 nibbles son mayores a 0x0600, por tanto es Ethernet II.

Datagrama:

- Versión protocolo: (4) → IPv4.
- Longitud cabecera (HLEN): (5) → 160 bits = 20 bytes.
- Tipo de servicio (TOS): (10) →00010000
    - (000) → Baja prioridad.
    - (1) → Bit D (Delay): Se desea un envío rápido.
    - (0) → Bit T (Throughput): No se busca un alto caudal de datos.
    - (0) → Bit R (Reliability): No se busca maximizar la confiabilidad de la transmisión.
    - (00) → No utilizados.
- Longitud total del datagrama: (01 48) → $0*16^3 + 1*16^2 + 4*16 + 8 = 328$ bytes.
- Identificación del datagrama: (00 00) → El ID IP 0 es un valor poco común pero es posible. De hecho, es característico, aunque no exclusivo, de sistemas Linux 2.4.x para el envío de segmentos UDP (Ref. post).
- Banderas + desplazamiento de fragmentación: (00 00) →00000000 00000000
    - Bits banderas (0-DF/NF-MF):
        - (0) → No se utiliza.
        - DF: (0) → Se permite la fragmentación.
        - MF: (0) → Es el último fragmento.
    - Bits despl. fragmentación: (0000000000000) → El paquete no está fragmentado.
- Tiempo de vida: (80) → 8*16 + 0*16 = 128 saltos.
- Tipo de protocolo del segmento/datagrama encapsulado: (11) → 1*16 + 1 = 17 , por lo tanto, es un datagrama UDP.
- Checksum de redundancia cíclica del datagrama: (d2 d2) → $13*16^3 + 2*16^2 + 13 * 16 + 2 = 53870$.

- Dirección IP de origen: (be 1f e5 ee) →10111110.00011111.11100101.11101110 = 190.31.229.238
- Dirección IP de destino: (c0 a8 02 0c) → 11000000.10101000.00000010.00001100 = 192.168.2.12, al ser una IP privada se podría intuir que es un paquete UDP que pertenece a una respuesta siendo enviada desde un router (MAC origen) a un host de su red (MAC destino) posterior al proceso de NAT de entrada.

Encabezado UDP (solo puertos para contextualizar):

- Puerto de origen: (00 43) → $0*16^3 + 0*16^2 + 4*16 + 3 = 67$, posiblemente se trate de un servidor DHCP. Esto refuerza la interpretación sobre la dirección IP destino.
- Puerto de destino: (00 44) →$0*16^3 + 0*16^2 + 4*16 + 4 = 68$, posiblemente se trate del cliente en la comunicación DHCP. Esto refuerza la interpretación sobre la dirección IP destino.

En resumen, esta trama (Ethernet II) encapsula un datagrama IP de 328 bytes, que requiere un servicio de baja prioridad, con envío rápido, sin un alto caudal de datos ni máxima confiabilidad. Además, el datagrama puede ser fragmentado en próximas transmisiones pero aún no lo está, puede dar hasta un máximo de 128 saltos de enrutamiento, contiene un datagrama UDP. Por último, según las direcciones de IP de origen y destino, en conjunto con los puertos de origen y destino se puede interpretar que es una comunicación a un servidor DHCP externo, con la respuesta ya ingresada a la red local transmitiéndose entre el router de la red local y un host de la misma, ya que la dirección IP de destino es privada, indicando que ya ocurrió el proceso de NAT de entrada.

2. Análisis de trama y datagrama B

Dado que los bytes proporcionados no incluyen el preámbulo (aa aa aa aa aa aa aa) ni el byte de inicio de trama (ab), se considera que los datos comienzan desde la dirección física (MAC) de destino.

Cuando se considera necesario es adopta la nomenclatura siguiente:

Campo: (nibble/s correspondientes en hex) → Interpretación o equivalente binario

Cabecera Ethernet

- Dirección física de destino: 00:19:db:7c:dd:0f
- Dirección física de origen: 00:1d:72:62:a2:bb.
- Tipo de protocolo del datagrama encapsulado: (08 00) → Protocolo IP. Los 4 nibbles son mayores a 0x0600, por tanto es Ethernet II.

Datagrama:

- Versión protocolo: (4) → IPv4.
- Longitud cabecera (HLEN): (5) → 160 bits = 20 bytes.
- Tipo de servicio (TOS): (00) →00000000
    - (000) → Baja prioridad.
    - (0) → Bit D (Delay): No se busca un envío rápido.
    - (0) → Bit T (Throughput): No se busca un alto caudal de datos.
    - (0) → Bit R (Reliability): No se busca maximizar la confiabilidad de la transmisión.
    - (00) → No utilizados.
- Longitud total del datagrama: (03 a1) →$0*16^3 + 3*16^2 + 10*16 + 1 = 929$ bytes.
- Identificación del datagrama: (17 1b) → $1*16^3 + 7*16^2 + 1*16 + 11 = 5915$.
- Banderas + desplazamiento de fragmentación: (40 00) →01000000 00000000
    - Bits banderas (0-DF/NF-MF):
        - (0) → No se utiliza.
        - DF: (1) → No se permite la fragmentación.
        - MF: (0) → Es el último fragmento, como la fragmentación no se permite también se interpreta que es el único.
    - Bits despl. fragmentación: (0000000000000) → El paquete no está fragmentado.
- Tiempo de vida: (80) → 8*16 + 0*16 = 128 saltos.
- Tipo de protocolo del segmento/datagrama encapsulado: (06) → 0*16 + 6 = 6, por lo tanto, es un segmento TCP.
- Checksum de redundancia cíclica del datagrama: (c8 c9) → $12*16^3 + 8*16^2 + 12 * 16 + 9 = 51401$.

- Dirección IP de origen: (c0 a8 02 0c) →11000000.10101000.00000010.00001100 = 192.168.2.12.
- Dirección IP de destino: (d1 55 c3 68) → 11010001.01010101.11000011.01101000 = 209.85.185.104, dado que esta dirección de IP es pública y la de origen es privada, se puede intuir que es una petición de algún tipo desde un host de una red local en el tramo hacia el router de dicha red para alcanzar algún servidor de la internet. Ambas direcciones MAC coinciden con las de la trama anterior pero en dirección contraria, por lo que se puede considerar que la comunicación se está dando en el mismo dominio de colisión.

Encabezado TCP (solo puertos para contextualizar):

- Puerto de origen: (cf af) → $12*16^3 + 15*16^2 + 10*16 + 15 = 53167$, este es un puerto efímero, lo que puede indicar que la comunicación TCP que se está dando podría ser algo como una petición HTTP desde una aplicación, como un navegador.
- Puerto de destino: (00 50) → $0*16^3 + 0*16^2 + 5*16 + 0 = 80$, este puerto se corresponde con una comunicación TCP.

En resumen, esta trama (Ethernet II) encapsula un datagrama IP de 929 bytes, que no requiere un servicio de alta prioridad, no requiere un envío rápido, ni un alto caudal de datos ni máxima confiabilidad. Además, el datagrama no puede ser fragmentado en próximas transmisiones, puede dar hasta un máximo de 128 saltos de enrutamiento y contiene un segmento TCP. Por último, según las direcciones de IP de origen y destino, en conjunto con los puertos de origen y destino se puede interpretar que es una comunicación a un servidor externo, dónde una petición está siendo enviada desde una aplicación hacia dicho servidor y esta se encuentra en el tramo entre el host y el router, ya que la dirección IP de origen es aún privada, indicando que no ocurrió el proceso de NAT de salida.