



EJERCICIOS DE REPASO DE ANÁLISIS DE TRÁFICO

1. Considerando las siguientes capturas de tráfico en una LAN, analice los siguientes casos, obtenga toda la información de la Capa N y saque conclusiones del funcionamiento del / de los protocolos de la Capa N (en esa captura), las funciones de red que cumple en la Capa N (en esa captura), así como los servicios que presta a la Capa N+1 (en esa captura) y aquellos que le requiere a la Capa N-1 (en esa captura), indicando los parámetros que para cada servicio o procesos intervienen en el transmisor, el receptor o ambos, si corresponde (en esa captura):

Trama#7

0000	ff ff ff ff ff ff f4 06	69 29 0d fb 08 00 45 00 i)....E.
0010	00 4e 40 88 00 00 80 11	75 4c c0 a8 01 7b c0 a8	.N@..... uL...{..
0020	01 ff 00 89 00 89 00 3a	5f a1 d8 8d 01 10 00 01: _.....
0030	00 00 00 00 00 00 20 46	48 46 41 45 42 45 45 43 F HFAEBEEC
0040	41 43 41 43 41 43 41 43	41 43 41 43 41 43 41 43	ACACACAC ACACACAC
0050	41 43 41 43 41 41 41 00	00 20 00 01	ACACAAA. . .

Trama#28

0000	e4 f8 9c b4 6c 39 f4 06	69 29 0d 06 08 00 45 0019.. i)....E.
0010	00 32 60 27 00 00 01 11	b6 db c0 a8 01 14 e0 00	.2`'.... ..
0020	00 fc d3 03 14 eb 00 1e	6e 0c 2e 22 00 00 00 01 n.."....
0030	00 00 00 00 00 00 04 77	70 61 64 00 00 01 00 01w pad.....

Trama#11

0000	c4 ea 1d 66 1a d4 e4 f8	9c b4 6c 39 08 00 45 00	...f.... ..19..E.
0010	00 3e 68 84 00 00 80 11	4e ca c0 a8 01 0f c0 a8	.>h.... N.....
0020	01 01 db 77 00 35 00 2a	95 53 02 1f 01 00 00 01	...w.5.* .S.....
0030	00 00 00 00 00 00 03 77	77 77 08 6d 73 66 74 6ew ww.msftn
0040	63 73 69 03 63 6f 6d 00	00 01 00 01	csi.com.

Trama#12

0000	c4 ea 1d 66 1a d4 e4 f8	9c b4 6c 39 08 00 45 00	...f.... ..19..E.
0010	00 41 76 af 00 00 80 11	40 9c c0 a8 01 0f c0 a8	.Av.... @.....
0020	01 01 ff e1 00 35 00 2d	ca f5 5e a2 01 00 00 015.- ..^.....
0030	00 00 00 00 00 00 03 77	77 77 08 6c 61 6e 61 63w ww.lanac
0040	69 6f 6e 03 63 6f 6d 02	61 72 00 00 01 00 01	ion.com. ar.....

Trama#30

Ethernet II, Src: Technico_66:1a:d4 (c4:ea:1d:66:1a:d4), Dst: IntelCor_b4:6c:39 (e4:f8:9c:b4:6c:39)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.15
User Datagram Protocol, Src Port: 53 (53), Dst Port: 56183 (56183)
Domain Name System (response)

[Request In: 11]

[Time: 0.024048000 seconds]

Transaction ID: 0x021f

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 4

Authority RRs: 0

Additional RRs: 0

> Queries

> Answers

Trama#36

0000	ff ff ff ff ff ff 84 10	0d 44 05 ac 08 06 00 01D.....
0010	08 00 06 04 00 01 84 10	0d 44 05 ac c0 a8 01 08D.....
0020	00 00 00 00 00 00 c0 a8	01 01



Trama#39

0000	00 0c 29 34 0b de 00 0c 29 c5 f6 9b 80 35 00 01	..)4....)....5..
0010	08 00 06 04 00 04 00 0c 29 c5 f6 9b 0a 01 01 0a).....
0020	00 0c 29 34 0b de 0a 01 01 64	..)4.... .d

Trama#78

0000	ff ff ff ff ff ff 00 05 02 71 fc db 81 00 00 14q.....
0010	00 24 aa aa 03 00 00 00 08 06 00 01 08 00 06 04	.\$.....
0020	00 01 00 05 02 71 fc db 83 97 14 48 ff ff ff ffq.. ...H....
0030	ff ff 83 97 14 fe 55 55 55 55 55 55 55 55 55UU UUUUUUUU

Trama#161

Internet Control Message Protocol		
0000	00 40 05 40 ef 24 00 60 08 9f b1 f3 81 00 00 20	..@.@\$..`
0010	08 00 45 00 05 dc 8a a4 20 00 40 01 82 b8 83 97	..E..... .@.....
0020	20 15 83 97 20 81 08 00 f0 e2 af 42 58 23 f9 1f BX#..
0030	23 38 24 bd 04 00 08 09 0a 0b 0c 0d 0e 0f 10 11	#8\$.....
0040	12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 !

Trama#562

0000	ff ff ff ff ff ff e4 f8 9c b4 6c 39 08 00 45 00l9..E.
0010	00 c6 18 84 00 00 80 11 9d 2f c0 a8 01 24 c0 a8/...\$..
0020	01 ff eb 25 19 f6 00 b2 0c e4 00 00 00 a6 00 00	...%.....
0030	00 06 00 00 00 00 00 00 00 08 00 00 00 18 4d 00M.
0040	63 00 4e 00 41 00 55 00 6e 00 69 00 71 00 75 00	c.N.A.U. n.i.q.u.
0050	65 00 49 00 64 00 0b 00 00 00 24 00 00 00 36 65	e.I.d... ..\$...6e
0060	63 64 34 34 61 39 2d 31 33 64 34 2d 34 62 36 37	cd44a9-1 3d4-4b67
0070	2d 61 63 36 34 2d 32 30 33 39 62 62 35 61 62 64	-ac64-20 39bb5abd
0080	34 34 01 00 00 00 18 4d 00 63 00 4e 00 41 00 55	44.....M .c.N.A.U
0090	00 6e 00 69 00 71 00 75 00 65 00 49 00 64 00 0b	.n.i.q.u .e.I.d..
00a0	00 00 00 24 00 00 00 37 38 32 30 63 31 38 63 2d	...\$...7 820c18c-
00b0	33 65 31 62 2d 34 63 37 35 2d 39 63 66 36 2d 36	3e1b-4c7 5-9cf6-6
00c0	31 62 64 62 37 61 63 37 37 39 61 01 7b de f7 bd	1bdb7ac7 79a.{...
00d0	00 00 00 00

Trama#2188

2188	20.742084	172.217.28.227	192.168.1.36	TCP	66 80 → 65019 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=14
Ethernet II, Src: Trendnet_2d:36:23 (d8:eb:97:2d:36:23), Dst: IntelCor_b4:6c:39 (e4:f8:9c:b4:6c:39)					
Destination: IntelCor_b4:6c:39 (e4:f8:9c:b4:6c:39)					
Source: Trendnet 2d:36:23 (d8:eb:97:2d:36:23)					
0000	e4 f8 9c b4 6c 39 d8 eb 97 2d 36 23 08 00 45 00l9..	..-6#..E.		
0010	00 34 e9 51 00 00 38 06 0d ea ac d9 1c e3 c0 a8	.4.Q..8.		
0020	01 24 00 50 fd fb 7d 5d dd 99 ee e6 16 ed 80 12	\$.P..}]		
0030	a7 94 dc ea 00 00 02 04 05 96 01 01 04 02 01 03		
0040	03 07	..			

Tramas#(varias)

2182 20.728707	192.168.1.36	172.217.28.227	TCP	66 65019 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
2188 20.742084	172.217.28.227	192.168.1.36	TCP	66 80 → 65019 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1430 S
2190 20.742436	192.168.1.36	172.217.28.227	TCP	54 65019 → 80 [ACK] Seq=1 Ack=1 Win=16384 Len=0
2192 20.742831	192.168.1.36	172.217.28.227	HTTP	340 GET /chrome/crlset/3067/crl-set-delta-3066-59196231364485582
2199 20.806741	172.217.28.227	192.168.1.36	TCP	60 80 → 65019 [ACK] Seq=1 Ack=287 Win=44032 Len=0
2200 20.806742	172.217.28.227	192.168.1.36	TCP	1484 [TCP segment of a reassembled PDU]
2201 20.806744	172.217.28.227	192.168.1.36	HTTP	751 HTTP/1.1 200 OK (text/html)
2202 20.807105	192.168.1.36	172.217.28.227	TCP	54 65019 → 80 [ACK] Seq=287 Ack=2128 Win=16384 Len=0
2206 20.816498	172.217.28.227	192.168.1.36	TCP	751 [TCP Spurious Retransmission] 80 → 65019 [PSH, ACK] Seq=1431
2208 20.816899	192.168.1.36	172.217.28.227	TCP	66 [TCP Dup ACK 2202#1] 65019 → 80 [ACK] Seq=287 Ack=2128 Win=1

> Frame 2202: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0

> Ethernet II, Src: IntelCor_b4:6c:39 (e4:f8:9c:b4:6c:39), Dst: Trendnet_2d:36:23 (d8:eb:97:2d:36:23)

> Internet Protocol Version 4, Src: 192.168.1.36, Dst: 172.217.28.227

> Transmission Control Protocol, Src Port: 65019 (65019), Dst Port: 80 (80), Seq: 287, Ack: 2128, Len: 0

0000	d8 eb 97 2d 36 23 e4 f8 9c b4 6c 39 08 00 45 00	...-6#.. ..l9..E.
0010	00 28 60 c2 40 00 80 06 0e 85 c0 a8 01 24 ac d9	.(^.@... ..\$..
0020	1c e3 fd fb 00 50 ee e6 18 0b 7d 5d e5 e9 50 10P.. ..}]..P.
0030	00 40 bb 86 00 00	..@....



2. PARA LAS TRAMAS ANTERIORES, SELECCIONE LAS OPCIONES CORRECTAS E INDIQUE LAS INCORRECTAS CON SUS FUNDAMENTOS:

- a. La trama#7 es una trama Ethernet II que encapsula un datagrama IPv6.
- b. La trama#7 es una trama de solicitud de resolución de dirección MAC para la IP 192.168.1.20.
- c. La trama#11 posee una dirección MAC destino del tipo UNICAST, encapsula un datagrama IP sin fragmentar, originado en el host 192.168.1.15, que encapsula una solicitud DNS para el sitio www.msftncsi.com, sobre un segmento UDP con puerto origen 56183.
- d. La trama#11 corresponde a los 80 bytes de una trama Ethernet II, que encapsulan un datagrama IP sin fragmentar, enviado por el host 192.168.1.15 al servidor 192.168.1.1, para realizar una consulta DNS encapsulada sobre un segmento UDP.
- e. La trama#12 encapsula un mensaje unicast de MAC generado por un host de la red IP 192.168.1.0/24 con socket destino 192.168.1.1:53
- f. La trama#12 encapsula un broadcast de MAC generado por un host con MAC e4.f8.9c.b4.6c.39, correspondiente al host 192.168.1.15, con destino a la dirección IP 192.168.1.1, que encapsula un segmento TCP.
- g. La trama#28 tiene MAC destino e4.f8.9c.b4.6c.39, MAC origen f4.06.69.29.0d.06 y encapsula un datagrama IP con host origen 192.168.1.20.
- h. La trama#28 indica un broadcast de MAC y encapsula un datagrama IP con: dirección origen 192.168.1.20 e IP destino multicast, datos capa 3 correspondientes a un servicio sin conexión, no confiable, sin control de flujo, con detección de errores opcional (utilizado en este caso y que tiene un valor de 6e.0c).
- i. La trama#28 es una trama unicast con IP origen 192.168.1.20. y es la respuesta a la trama#7.
- j. La trama#30 es la respuesta a la solicitud DNS de la trama#11
- k. La trama#30 indica que el nodo 192.168.1.15 ha enviado una consulta estándar DNS para el sitio www.msftncsi.com.
- l. La trama#30 señala que el host 192.168.1.1 brinda el servicio DNS al segmento IP respectivo y se identifica en la LAN con dirección MAC c4.ea.1d.66.1a.d4.
- m. La trama#36 es una trama Ethernet II que encapsula un datagrama IP (0800).
- n. La trama#36 es una trama de solicitud de resolución de dirección MAC para la IP 192.168.1.1.
- o. La trama#36 es una trama de solicitud de resolución de dirección MAC para la IP 192.168.1.1. y la respuesta es dada en la trama#39.
- p. La trama#39 tiene MAC destino 00.0c.29.34.0b.de, MAC origen 00.0c.29.c5.f6.9b y encapsula un datagrama IP (0800) con host destino 10.1.1.100.
- q. La trama#39 tiene MAC destino 00.0c.29.34.0b.de, MAC origen 00.0c.29.c5.f6.9b y encapsula un protocolo de resolución de dirección IP desconocida que le corresponda a la MAC origen.
- r. La trama#78 posee una dirección MAC origen del tipo UNICAST, encapsula un datagrama IP sin fragmentar, originado en el host 131.151.20.72, que encapsula una solicitud DNS para el sitio www.google.com.ar, sobre un segmento UDP con puerto origen 56183.
- s. La trama#78 indica que el nodo 131.151.20.72 ha enviado una solicitud ARP consultando la MAC que le corresponde al host IP 131.151.20.254.
- t. La trama#161 es la respuesta a la solicitud DNS de la trama#78.
- u. La trama#161 Ethernet II corresponde a los 1.500 bytes de un datagrama IP fragmentado que proporciona direccionamiento a un paquete ICMP, enviado por el host 131.151.32.21 al host 131.151.32.129.



- v. La trama#161 señala que el host 131.151.32.21 pertenece a la VLAN 32, encapsula el primer paquete IP fragmentado con una solicitud de ECHO correspondiente al protocolo ICMP y se descartará luego de 64 saltos, en caso de no llegar a destino.
- w. La trama#562 encapsula un broadcast de MAC generado por un host de la red 192.168.1.0/24 con IP destino a la dirección de broadcast de esa red.
- x. La trama#562 encapsula un broadcast de MAC generado por un host con MAC e4.f8.9c.b4.6c.39, perteneciente a la red 192.168.1.0/24, con destino a la dirección IP 192.168.1.1.
- y. La trama#562 encapsula un broadcast de MAC generado por el host 192.168.1.36 con IP destino a la dirección 192.168.1.255, sin fragmentar, que encapsula un segmento UDP con 170 bytes de datos.
- z. La trama#2188 indica que el servidor HTTP con IP 172.217.28.227 confirma la recepción de solicitud de conexión del host 192.168.1.36 y propone un valor de tamaño de ventana de 42.900 bytes y tamaño máximo de segmento de 1.430 bytes.

Para el caso de Tramas#(varias):

- aa. Las tramas #2182, #2188 y #2190 encapsulan 3 segmentos, respectivamente, el establecimiento de conexión entre el host 192.168.1.36 y el servidor 172.217.28.227, que acuerdan un tamaño de ventana de 42.900 bytes.
- bb. La trama#2202 indica que el servidor HTTP con IP 172.217.28.227 confirma la recepción del segmento con número de secuencia SEQ=287 e identifica, con un valor de 2128, la posición de los datos del segmento en el flujo de datos del host 192.168.1.36.
- cc. La trama#2202 es una confirmación del segmento TCP encapsulado en la trama#2201, siempre y cuando la trama #2201 tuviera un valor SEQ=1431 y el segmento TCP transmitiera 697 bytes de datos.

3. RESUELVA LOS SIGUIENTES EJERCICIOS:

- a. ¿Cuál es **el número mínimo de Bytes** con que debe ejecutarse la aplicación PING extendido para que se produzca una fragmentación de un datagrama IP sobre Ethernet, con **44 paquetes**? Demuestre la fundamentación de su estimación o cálculo (al reverso de la hoja).

RESPUESTA: Bytes.

- a. ¿Cuál es **el número mínimo de Bytes** con que debe ejecutarse la aplicación PING extendido para que se produzca una fragmentación de un datagrama IP sobre Ethernet, con **35 paquetes**? Demuestre la fundamentación de su estimación o cálculo (al reverso de la hoja).

RESPUESTA: Bytes.

- b. ¿Cuál es **el número de paquetes IP** que se generan en una red con una MTU de 1000 bytes si la aplicación de red HTTP encapsula 125.990 bytes en el protocolo de capa 4? Demuestre la fundamentación de su estimación o cálculo (al reverso de la hoja).

RESPUESTA: paquetes IP.



c. Indique ¿qué valores tendrá el campo FLAGS en el primero, penúltimo y último paquete en caso de fragmentación IP?

FLAGS: PRIMER PAQUETE: ...0x.....

PENÚLTIMO PAQUETE: ...0x..... ÚLTIMO PAQUETE: ...0x.....

d. En base a la siguiente captura, RESPONDA:

No.	Time	Source	Destination	Protocol	Length	Info
17	8.026826	192.168.1.6	192.168.1.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=129)
18	8.026854	192.168.1.6	192.168.1.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=129)

▣ Frame 17: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 1

▣ Ethernet II, Src: Azurewav_14:e1:21 (00:25:d3:14:e1:21), Dst: Zte_7b:bf:73 (9c:d2:4b:7b:bf:73)

▣ Internet Protocol Version 4, Src: 192.168.1.6 (192.168.1.6), Dst: 192.168.1.1 (192.168.1.1)

Version: 4

Header Length: 20 bytes

▣ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Tran

Total Length: 1500

Identification: 0x129b (4763)

▣ Flags: 0x01 (More Fragments)

Fragment offset: 2960

Time to live: 128

Protocol: ICMP (1)

▣ Header checksum: 0x7dbc [validation disabled]

Source: 192.168.1.6 (192.168.1.6)

Destination: 192.168.1.1 (192.168.1.1)

[Source GeoIP: Unknown]

0000	9c d2 4b 7b bf 73 00 25 d3 14 e1 21 08 00 45 00	..K{.s.% ...!..E.
0010	05 dc 12 9b 21 72 80 01 7d bc c0 a8 01 06 c0 a8!r.. }.....
0020	01 01 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	..ijklmn opqrstuv
0030	77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f	wxyzdefghijklmno

- 1) ¿Cómo se relacionan Header Length y Total Length? Responda con precisión y exactitud.
- 2) ¿En qué procesos intervienen los campos de Id, Flags y Fragment Offset, en el transmisor y en el receptor? Describa un ejemplo en base a una captura anterior o agregue uno nuevo.
- 3) ¿Para qué sirve el campo Time to live con valor 128?