

Conjunto de problemas 3

0000 1A 00 00 33 33 33 1A 00 00 77 77 77 08 00 4 5 00

MAC destino MAC origen Ethe-type (ip) Ipv4 long TOS

0010 00 28 00 2A 0 0 00 40 06 65 92 C0 A8 01 07 50 50

Long Idpkt F Offset TTL (TCP) Checksum IP orig (192.168.1.7) IP Dest
(80.80.3.21)

0020 03 15 3B 6D 00 6E 00 00 00 2A 00 00 00 00 5 0 02

Puer.O(15213) Puer.D.(110) N° sec. N° ACK HL nada+flags SYN

0030 20 00 3E C9 00 00

Win Checksum Urg Point. **POP3.**

192.168.1.7 --> 80.80.3.21:POP3 TCP SYN (0000002A)

0000 1A 00 00 33 33 33 1A 00 00 55 55 55 08 00 4 5 00

MAC destino MAC origen Ethe-type (ip) Ipv4 long TOS

0010 00 28 00 2A 0 0 00 33 06 5E E3 C0 A8 01 05 64 01

Long Idpkt F Offset TTL (TCP) Checksum IP orig (192.168.1.5) IP Dest
(100.1.3.21)

0020 03 15 00 0A 00 50 00 00 00 64 00 00 00 00 5 0 02

Puer.O(10) Puer.D.(80) N° sec. N° ACK HL nada+flags SYN

0030 20 00 66 61 00 00

Win Checksum Urg Point. **Web.**

192.168.1.5:10 --> 100.1.3.21:Web TCP SYN

0000 1A 00 00 33 33 33 1A 00 00 55 55 55 08 00 4 5 00

	MAC destino	MAC origen	Ethe-type (ip)	Ipv4	long	TOS
0010	00 38 00 2A	0 0 00 33 11	9F D8	C0 A8 01 05		25 04
	Long	Idpkt	F	Offset	TTL (UDP)	Checksum
0020	01 02	00 0A 00 50	00 24	55 EE	6C 73 64 51 3	2 79
	Puer.O(10)	Puer.D.(80)	Long	checksum		Datos
0030	33 49 78 4D	79 73 58 63	36 31 53 68	4B 65 79 4E		

0040 6D 31 44 43 41 3D **UDP Web**

192.168.1.5:10 --> 37.4.1.2: UDP: 80

0000	1A 00 00 77 77 77	1A 00 00 33 33 33	08 00	4	5	00
	MAC destino	MAC origen	Ethe-type (ip)	Ipv4	long	TOS
0010	00 28 8A 5E	0 0 00 36 06	E5 5D	50 50 03 15	C0 A8	
	Long	Idpkt	F	Offset	TTL (TCP)	Checksum
					IP orig (80.80.3.21)	IP Dest (192.168.1.7)
0020	01 07	00 6E	3B 6D	00 75 4E 07	00 00 00 2B	5 0 12
	Puer.O(110)	Puer.D.(15213)	Nº sec.	Nº ACK	HL	nada+flags ACK+SYN
0030	20 00	F0 3B	00 00			
	Win	Checksum	Urg	Point.	POP3.	

192.168.1.7:pop3 --> 80.80.3.21:15213 ACK (0000002B) + SYN (00754E07)

0000	1A 00 00 55 55 55	1A 00 00 33 33 33	08 00	4	5	00
	MAC destino	MAC origen	Ethe-type (ip)	Ipv4	long	TOS
0010	00 28 79 FF	0 0 00 30 06	E8 0D	64 01 03 15	C0 A8	
	Long	Idpkt	F	Offset	TTL (TCP)	Checksum
					IP orig (100.1.3.21)	IP Dest (192.168.1.5)
0020	01 05	00 50	00 0A	00 00 00 00	00 00 00 00	5 0 04
	Puer.O(80)	Puer.D.(10)	Nº sec.	Nº ACK	HL	nada+flags RST

0030 20 00 66 C3 00 00

Win Checksum Urg Point.

100.1.3.21:web --> 192.168.1.5:10 RST

0000 1A 00 00 33 33 33 1A 00 00 77 77 77 08 00 4 5 00

MAC destino MAC origen Ethertype (ip) Ipv4 long TOS

0010 00 28 00 2B 0 0 00 40 06 65 91 C0 A8 01 07 50 50

Long Idpkt F Offset TTL (TCP) Checksum IP orig (192.168.1.7) IP Dest (80.80.3.21)

0020 03 15 3B 6D 00 6E 00 00 00 2B 00 75 4E 08 5 0 10

Puer.O(15213) Puer.D.(110) N° sec. N° ACK HL nada+flags ACK

0030 20 00 F0 3C 00 00

Win Checksum Urg Point. **POP3.**

192.168.1.7:15213 --> 80.80.3.21:POP3 TCP ACK (00754E08) (0000002B)

Pregunta 3.1

Protocolos por nivel:

Enlace: IP

Red: Ipv4 con TCP y UDP

Transporte: Puerto destino Web (pruebas) y POP3

192.168.1.7 --> 80.80.3.21:POP3 TCP SYN (0000002A)

1A 00 00 77 77 77 -> 1A 00 00 33 33 33

192.168.1.5:10 --> 100.1.3.21:Web TCP SYN

1A 00 00 55 55 55 -> 1A 00 00 33 33 33

192.168.1.5:10 --> 37.4.1.2: UDP: 80

1A 00 00 55 55 55 -> 1A 00 00 33 33 33

80.80.3.21:pop3 --> 192.168.1.7:15213 ACK (0000002B) + SYN (00754E07)

1A 00 00 33 33 33 -> 1A 00 00 77 77 77

100.1.3.21:web --> 192.168.1.5:10 RST

1A 00 00 33 33 33 -> 1A 00 00 55 55 55

192.168.1.7:15213 --> 80.80.3.21:POP3 TCP ACK (00754E08) (0000002B)

1A 00 00 77 77 77 -> 1A 00 00 33 33 33

Pregunta 3.2

La aplicación que genera los paquetes:

192.168.1.7 --> 80.80.3.21:POP3 TCP SYN (0000002A)

1A 00 00 77 77 77 -> 1A 00 00 33 33 33

user agent, un programa de correo lector, que pide conexión con POP3.

192.168.1.5:10 --> 100.1.3.21:Web TCP SYN

1A 00 00 55 55 55 -> 1A 00 00 33 33 33

Una aplicación que emite desde el puerto 10, mmmh

192.168.1.5:10 --> 37.4.1.2: UDP: 80

1A 00 00 55 55 55 -> 1A 00 00 33 33 33

Una aplicación que emite desde el puerto 10, mmmh

192.168.1.7:pop3 --> 80.80.3.21:15213 ACK (0000002B) + SYN (00754E07)

1A 00 00 33 33 33 -> 1A 00 00 77 77 77

Respuesta del servidor de correo POP3.

100.1.3.21:web --> 192.168.1.5:10 RST

1A 00 00 33 33 33 -> 1A 00 00 55 55 55

El protocolo TCP informa que ese puerto no está activo.

192.168.1.7:15213 --> 80.80.3.21:POP3 TCP ACK (00754E08) (0000002B)

1A 00 00 77 77 77 -> 1A 00 00 33 33 33

user agent, un programa de correo lector, que manda ACK de conexión establecida.

Pregunta 3.3

Ordenadores, red privada:

192.168.1.7 (mac: 1A 00 00 77 77 77) PC7

192.168.1.5 (mac: 1A 00 00 55 55 55) PC5

192.168.1.x (mac 1A 00 00 33 33 33) ROUTER.

100.1.3.21 fuera de la red, no es servidor de web.

37.4.1.2 fuera de la red, no es servidor web de udp.

80.80.3.21:POP3 fuera de la red.

Pregunta 3.4

Red privada, cliente 192.168.1.7 (user agent).

Red externa servidor 80.80.3.21

Pregunta 3.5

Una conexión TCP de 192.168.1.7 hacia 80.80.3.21 servicio POP3.

Resto son ataques a varias IP's al puerto 80 con TCP y UDP. La respuesta de TCP de puerto no disponible.

Pregunta 3.6

2 conexiones TCP.

- Pop3.

- Web (sin éxito)

Pregunta 3.7

Establecimiento completo 1, el de POP3.

```

0000  1A 00 00 33 33 33  1A 00 00 77 77 77  08 00  4  5  00
      MAC destino      MAC origen      Ethe-type (ip)      Ipv4 long TOS

0010  00 28 00 2A 0 0 00  33 06  FA 8E  53 01 03 0C  35 01
      Long Idpkt F Offset TTL (TCP) Checksum IP orig (83.1.3.12) IP Dest (53.1.3.10)

0020  02 0A 4E 20 00 19 00 00 00 2A 00 00 00 00  5 0 02
      Puer.O(20000) Puer.D.(25) N° sec. N° ACK HL nada+flags SYN

0030  20 00 B4 67 00 00
      Win Checksum Urg Point. SMTP.

```

83.1.3.12:20000 --> 53.1.2.10:SMTP TCP SYN (0000002A)

```

0000  1A 00 00 33 33 33  1A 00 00 77 77 77  08 00  4  5  00
      MAC destino      MAC origen      Ethe-type (ip)      Ipv4 long TOS

0010  00 28 00 2A 0 0 00  33 06  CD 66  82 14 01 21  35 01
      Long Idpkt F Offset TTL (TCP) Checksum IP orig (130.20.1.33) IP Dest (53.1.3.10)

0020  02 0A 4E 20 00 19 00 00 00 2A 00 00 00 00  5 0 02
      Puer.O(20000) Puer.D.(25) N° sec. N° ACK HL nada+flags SYN

0030  20 00 87 3F 00 00
      Win Checksum Urg Point.

```

130.20.1.33:20000 --> 53.1.2.10:SMTP TCP SYN (0000002A)

```

0000  1A 00 00 33 33 33  1A 00 00 77 77 77  08 00  4  5  00
      MAC destino      MAC origen      Ethe-type (ip)      Ipv4 long TOS

0010  00 28 00 2A 0 0 00  33 06  37 37  17 64 02 01  35 01
      Long Idpkt F Offset TTL (TCP) Checksum IP orig (23.100.2.1) IP Dest (53.1.3.10)

0020  02 0A 4E 20 00 19 00 00 00 2A 00 00 00 00  5 0 02
      Puer.O(20000) Puer.D.(25) N° sec. N° ACK HL nada+flags SYN

0030  20 00 F1 0F 00 00

```

Win Checksum Urg Point.

23.100.2.1:20000 --> 53.1.2.10:SMTP TCP SYN (0000002A)

0000 1A 00 00 77 77 77 1A 00 00 33 33 33 08 00 4 5 00
MAC destino MAC origen Ethe-type (ip) Ipv4 long TOS

0010 00 28 8A 5E 0 0 00 3F 06 64 5A 35 01 02 0A 53 01
Long Idpkt F Offset TTL (TCP) Checksum IP orig (53.1.2.10) IP Dest (83.1.3.12)

0020 03 0C 4E 20 00 19 00 75 4E 07 00 00 00 2B 5 0 12
Puer.O(20000) Puer.D.(25) N° sec. N° ACK HL nada+flags ACK+SYN

0030 20 00 65 DA 00 00
Win Checksum Urg Point. **POP3.**

53.1.2.10:20000 -->83.1.3.12:25 ACK (0000002B) + SYN (00754E07)

0000 1A 00 00 33 33 33 1A 00 00 77 77 77 08 00 4 5 00
MAC destino MAC origen Ethe-type (ip) Ipv4 long TOS

0010 00 28 00 2A 0 0 00 33 06 EA 97 64 01 02 03 35 01
Long Idpkt F Offset TTL (TCP) Checksum IP orig (100.1.2.3) IP Dest (53.1.3.10)

0020 02 0A 4E 20 00 19 00 00 00 2A 00 00 00 00 5 0 02
Puer.O(20000) Puer.D.(25) N° sec. N° ACK HL nada+flags SYN

0030 20 00 A4 70 00 00
Win Checksum Urg Point.

100.1.2.3:2000 --> 53.1.2.10:SMTP TCP SYN (0000002A)

Pregunta 3.8

Protocolos por nivel:

Enlace: IP

Red: TCP, ipv4

Transporte: puerto destino SMTP.

Pregunta 3.9

Pertenecen a un servidor de correo saliente, SMTP.

Enviados por varios clientes, al mismo servidor. Una respuesta del servidor a un cliente.

Pregunta 3.10

83.1.3.12:20000 --> 53.1.2.10:SMTP TCP SYN (0000002A)
1A 00 00 77 77 77 -> 1A 00 00 33 33 33

130.20.1.33:20000 --> 53.1.2.10:SMTP TCP SYN (0000002A)
1A 00 00 77 77 77 -> 1A 00 00 33 33 33

23.100.2.1:20000 --> 53.1.2.10:SMTP TCP SYN (0000002A)
1A 00 00 77 77 77 -> 1A 00 00 33 33 33

53.1.2.10:25 -->83.1.3.12:20000 ACK (0000002B) + SYN (00754E07)
1A 00 00 33 33 33 -> 1A 00 00 77 77 77

100.1.2.3:2000 --> 53.1.2.10:SMTP TCP SYN (0000002A)
1A 00 00 77 77 77 -> 1A 00 00 33 33 33

Pregunta 3.11

Todas son conexiones diferentes salvo el cuarto y el primero.

Pregunta 3.12

Tras un ping se tiene en caché ARP la MAC del router de salida. También se sabe la IP porque ya ha consultado al DNS.

Tras ENTER:

	MAC-orig	MAC-dest	IP-origen:	IP-destino:	P-orig	P-dest
pkt1	00:00:1A:00:11:11	00:3F:00:00:33:33	192.168.1.34	173.194.41.216	Xxx	80
Más	Ip	TCP	SYN	(nº sec YYY)		
pkt2	00:3F:00:00:33:33	00:00:1A:00:11:11	173.194.41.216	192.168.1.34	80	Xxx
Más	IP	TCP	SYN + ACK(YYY)	(nº sec ZZZ)		
pkt3	00:00:1A:00:11:11	00:3F:00:00:33:33	192.168.1.34	173.194.41.216	Xxx	80
Más	Ip	TCP	ACK (ZZZ+1)			
pkt4	00:00:1A:00:11:11	00:3F:00:00:33:33	192.168.1.34	173.194.41.216	Xxx	80
Más	Ip	TCP	(nº sec YYY+N)	GET / HTTP		

pkt5	00:3F:00:00:33:33	00:00:1A:00:11:11	173.194.41.216	192.168.1.34	80	Xxx
Más	IP	TCP	ACK(YYY+1)	(nº sec ZZZ+M) HTML		

Pregunta 3.13

```

000028  00 A0 C5 9D 52 00  00 0C      93 45 2D 74 08 00      4    5    10
          MAC destino      MAC origen      Ethe-type (ip)      IPv4  long  TOS

000038  00 3C 44 39 4 0 00  40  06  0D AC      C0 A8 01 0C      82 CE
          Long  Idpkt  F Offset TTL (TCP)  Checksum  IP orig (192.168.1.12)  IP Dest
(130.206.164.68)

000048  A4 44 4E 20  00 17  95 9E  D2 87 00 00 00 00  A  0 02
          Puer.O(59702) Puer.D.(23)  N° sec.      N° ACK      HL  nada+flags SYN

000058  FF FF  E8 F5      00 00  02 04  05 B4 01 03 03 00 01 01
          Win  Checksum      Urg Point. DATOS

000068  08 0A 7E F5 CB 7F 00 00 00 00

```

192.168.1.12:59702 --> 130.206.164.68:TELNET TCP SYN

a) Es un paquete TCP. Posición 00000038, valor 06 de protocolo transporte.

Pregunta 3.14

Son ciertas:

- a) El paquete transporta datos de nivl de aplicación (sí. TELNET)
- b) El cliente es la dirección IP de rango privado: sí. **192.168.1.12:59702**
- e) El paquete ha sido generado por una sesión de Telnet. Sí, puerto 23 destino.
- g) Por ser destino fuera de la red, la MAC destino es del router. Según la tabla de direcciones del ieee, la 00A0C5 es de ZYXEL Communication. NO ES CISCO.

Resto: NO.

Pregunta 3.15

IP (0800)

UDP (puerto 0x11=17)

Iporigen=0XC0A8 01FE = 192.168.1.254: 53 (DNS 0X0035)

Ipdestino= 0XC0A80124 = 192.168.1.36: 50499 (0XC543)

Por lo que:

b) es un paquete UDP, respuesta de una consulta DNS (53).

web1.skype.com 9D 38 72 69 (157.56.114.105)

ns1.skype.net D4 08 A3 62 (212.8.163.98)

Pregunta 3.16

Cierto:

a) El paquete transporta datos de nivel de aplicación (DNS respuesta)

e) El paquete lo ha enviado un servidor del servicio DNS.

Pregunta 3.17

Paquete TCP, 130.206.160.97:50551 --> 130.206.166.108: 110 (POP3) Nª sec. 09 71 cc 3c

El campo ACK del paquete que confirme la entrega de este paquete será: 0971CC3D

Pregunta 3.18

b) Sólo los extremos de la comunicación T1 y T5, ya que el resto sólo leen hasta nivel de red.

Pregunta 3.19