



UNIVERSITAT_{DE}
BARCELONA

Xarxes

Quart lliurament

Arnau Gris Garcia, Eric Duque Martín i Joel Otero Martín

Pràctica 4 de Xarxes

13/12/2020

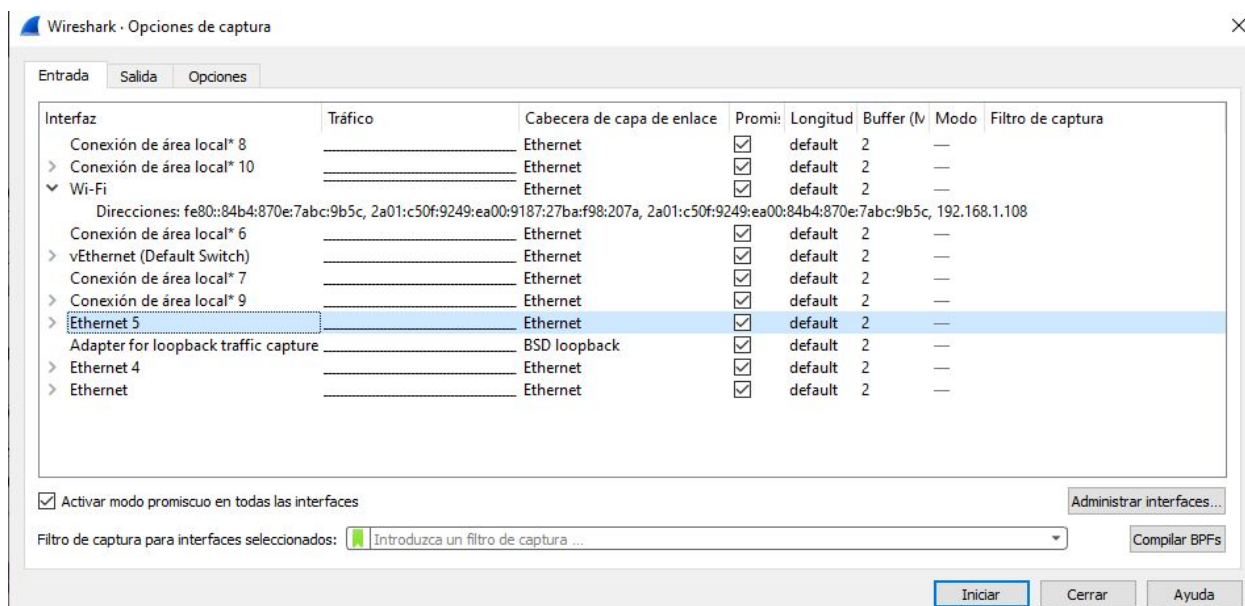
Objectius de la pràctica

En aquesta pràctica es pretén conèixer com funcionen les diferents DPU i la seva encapsulació, per això es realitzen diferents exercicis:

- Primer es proposen una sèrie de qüestions sobre les adreces MAC i les IP públiques associades.
- Al primer exercici s'utilitza el programa Wireshark per filtrar la informació referent a la nostra IP.
- A l'exercici número 2 es vol conèixer com funciona el protocol DNS, quins paquets intercanvia aquest, la seva relació amb el protocol TCP i el funcionament d'aquest mateix.
- Al tercer exercici es presenta el protocol ICMP i el seu funcionament.
- A l'última qüestió s'utilitza el programa Cisco Packet Tracer per configurar una NAT entre dues xarxes.

Preguntes

Visualitzeu les característiques de cada interfície clicant al botó de “details”. Indiqueu que teniu i expliqueu detalladament que apareix.



En obrir la finestra podem veure totes les connexions a internet que tenim disponibles en la nostra xarxa local. Podem observar diferents paràmetres que defineixen una interfície.

El tràfic mostra un petit gràfic sobre les dades que arriben.

En la capçalera de capa d'enllaç podem veure quin tipus utilitza, en la imatge veiem Ethernet i BSD loopback.

Si cliquem en Wi-Fi, per exemple, se'ns mostra les direccions IPV6 i IPV4.

Seleccioneu la interfície d'Ethernet. Apunteu l'adreça MAC que surt i executeu des de consola un `ipconfig /all`. Identifiqueu la IP associada a aquesta MAC. Descriviu curosament els detalls a l'informe.

Seleccionem la interfície Ethernet del nostre Wi-Fi.

Tenim que estem enviant dades des de la direcció MAC: **d0:37:45:a9:00:86**

449	4.706592	192.168.1.108	192.168.1.1	DNS	92 Standard query 0x9527 AAAA geo.prod.do.dsp.mp.microsoft.com
456	4.720098	fe80::84b4:870e:7ab...	fe80::5edc:96ff:fec...	DNS	104 Standard query 0x3250 AAAA ipv6.msftconnecttest.com

Frame 449: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{A25B923C-04C0-45BB-A9D2-D9AB4EFC909A}, id 0
Ethernet II, Src: Tp-LinkT_a9:00:86 (d0:37:45:a9:00:86), Dst: Arcadyan_cc:cc:11 (5c:dc:96:cc:cc:11)
> Destination: Arcadyan_cc:cc:11 (5c:dc:96:cc:cc:11)
> Source: Tp-LinkT_a9:00:86 (d0:37:45:a9:00:86)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.108, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 55609, Dst Port: 53

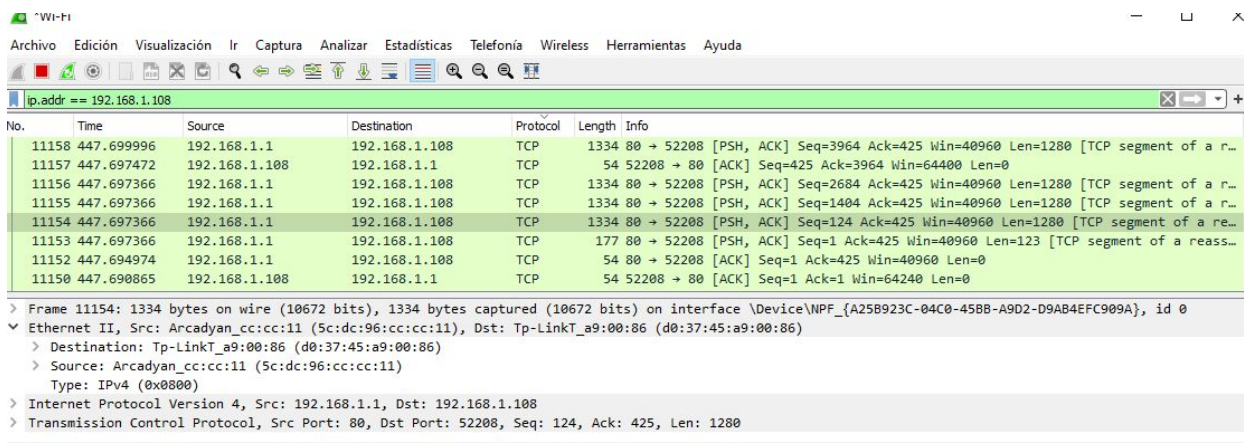
00	5c	dc	96	cc	cc	11	d0	37	45	a9	00	86	08	00	45	00	...	7	EE		
10	00	4e	d7	05	00	00	80	11	df	db	c0	a8	01	6c	c0	a8	...	N1		
20	01	01	d9	39	00	35	00	3a	86	6c	95	27	01	00	00	01	...	9	51	
30	00	00	00	00	00	00	03	67	65	6f	04	70	72	6f	64	02	...	g	eo	prod	
40	64	6f	03	64	73	70	02	6d	70	09	6d	69	63	72	6f	73	...	do	dsp	m	micro
50	6f	66	74	03	63	6f	6d	00	00	1c	00	01					...	oft	com	

Si fem "`ifconfig /all`" veiem que la direcció MAC correspon a la del nostre ordinador:

Adaptador de LAN inalámbrica Wi-Fi:	
Sufijo DNS específico para la conexión.	: home
Descripción	: TP-Link Wireless Nano USB Adapter
Dirección física.	: D0-37-45-A9-00-86
DHCP habilitado	: sí
Configuración automática habilitada	: sí
Dirección IPv6	: 2a01:c50f:9249:ea00:84b4:870e:7abc:9b5c(Preferido)
Dirección IPv6 temporal.	: 2a01:c50f:9249:ea00:9187:27ba:f98:207a(Preferido)
Vínculo: dirección IPv6 local.	: fe80::84b4:870e:7abc:9b5c%18(Preferido)
Dirección IPv4.	: 192.168.1.108(Preferido)
Máscara de subred	: 255.255.255.0
Concesión obtenida.	: miércoles, 2 de diciembre de 2020 12:45:55
La concesión expira	: domingo, 9 de enero de 2157 21:26:30
Puerta de enlace predeterminada	: fe80::5edc:96ff:fecc:cc11%18
	192.168.1.1
Servidor DHCP	: 192.168.1.1
IAID DHCPv6	: 248526661
DUID de cliente DHCPv6.	: 00-01-00-01-25-8C-2D-1D-00-26-18-F4-51-95
Servidores DNS.	: fe80::5edc:96ff:fecc:cc11%18
	192.168.1.1
NetBIOS sobre TCP/IP.	: habilitado
Lista de búsqueda de sufijos DNS específicos de conexión:	
	home

La ip associada a aquesta MAC és: **192.168.1.108**

Exercici 1:



The screenshot shows the Wireshark interface with a packet capture filter set to 'ip.addr == 192.168.1.108'. The packet list shows several TCP segments. The selected packet (No. 11154) is expanded, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
11158	447.699996	192.168.1.1	192.168.1.108	TCP	1334	80 → 52208 [PSH, ACK] Seq=3964 Ack=425 Win=40960 Len=1280 [TCP segment of a r...
11157	447.697472	192.168.1.108	192.168.1.1	TCP	54	52208 → 80 [ACK] Seq=425 Ack=3964 Win=64400 Len=0
11156	447.697366	192.168.1.1	192.168.1.108	TCP	1334	80 → 52208 [PSH, ACK] Seq=2684 Ack=425 Win=40960 Len=1280 [TCP segment of a r...
11155	447.697366	192.168.1.1	192.168.1.108	TCP	1334	80 → 52208 [PSH, ACK] Seq=1404 Ack=425 Win=40960 Len=1280 [TCP segment of a r...
11154	447.697366	192.168.1.1	192.168.1.108	TCP	1334	80 → 52208 [PSH, ACK] Seq=124 Ack=425 Win=40960 Len=1280 [TCP segment of a re...
11153	447.697366	192.168.1.1	192.168.1.108	TCP	177	80 → 52208 [PSH, ACK] Seq=1 Ack=425 Win=40960 Len=123 [TCP segment of a reass...
11152	447.694974	192.168.1.1	192.168.1.108	TCP	54	80 → 52208 [ACK] Seq=1 Ack=425 Win=40960 Len=0
11150	447.690865	192.168.1.108	192.168.1.1	TCP	54	52208 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

Frame 11154: 1334 bytes on wire (10672 bits), 1334 bytes captured (10672 bits) on interface \Device\NPF_{A25B923C-04C0-458B-A9D2-D9AB4EFC909A}, id 0

Ethernet II, Src: Arcadyan_cc:cc:11 (5c:dc:96:cc:cc:11), Dst: Tp-LinkT_a9:00:86 (d0:37:45:a9:00:86)

Destination: Tp-LinkT_a9:00:86 (d0:37:45:a9:00:86)

Source: Arcadyan_cc:cc:11 (5c:dc:96:cc:cc:11)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.108

Transmission Control Protocol, Src Port: 80, Dst Port: 52208, Seq: 124, Ack: 425, Len: 1280

1. Com es descriu la vostra adreça MAC?

La nostra adreça MAC és descrita com abans, d0:37:45:a9:00:86. Ja hem vist que correspon a la IP física del nostre ordinador.

2. A la adreça MAC hi han dues parts clarament diferenciades. A que corresponen?

Adreça MAC: (d0:37:45:a9:00:86)

En el nostre cas tenim aquestes dues parts:

1. d0:37:45... (Correspon a la primera meitat de l'adreça Mac)
2. ...9:00:86 (Correspon a la segona meitat de l'adreça Mac)

La primera meitat correspon al fabricant del dispositiu. La segona meitat de l'adreça MAC correspon al número de sèrie. Les adreces MAC són úniques.

3. Compara el que apareix amb el que surt amb un ipconfig/all.

En el "ipconfig /all" com ja hem vist, veiem aquesta adreça MAC: D0-37-45-A9-00-86

4. Repassa els diferents camps que apareixen a la capçalera IP i amb l'ajut dels llibres i/o Internet identifica que fa cada un dels camps.

- **Versió (4 bits):** Indica la versió IP, pot variar entre (0100) o (0110) que corresponent a IPv4 i IPv6.

- **Longitud capçalera (4 bits):** Representa la longitud de capçalera, està representada per paraules de 32 bits. El seu valor mínim són 5 paraules i el màxim 15.
- **Tipus de servei (8 bits):** Indica una sèrie de paràmetres sobre la qualitat del servei desitjada durant el trànsit d'una xarxa. Algunes xarxes ofereixen prioritat de serveis, considerant determinat tipus de paquets més importants que altres.
- **Longitud total (16 bits):** La mida total del datagrama en octets.
- **Identificador (16 bits):** Identificador únic del datagrama. S'utilitza quan el datagrama ha de ser fragmentat, per poder distingir els fragments d'un datagrama d'altres.
- **Flags (3 bits):** utilitzat només per especificar els valors relacionats a la fragmentació de paquets. Els tres bits són:
 - Bit 0: Reservat, ha de ser 0.
 - Bit 1: 0 = divisible, 1 = no divisible
 - Bit 2: 0 = últim fragment, 1 = Fragment intermedi (venen més fragments).
- **Posició de fragments (13 bits):** En paquets fragmentats indica la posició, en unitats de 64 bits, que ocupa el paquet actual dins del datagrama inicial.
- **Temps de vida (TTL, 8 bits):** Indica el màxim nombre d'enrutadors que un paquet pot travessar. Per cada node aquest nombre va disminuint, si arriba a 0, el paquet es descarta.
- **Protocol (8 bits):** Indica el protocol de les capes superiors a les quals ha d'entregar-se el paquet
- **Suma de control de capçalera (16 bits):** 'Checksum' per control de corrupció de la capçalera. Es recalcula cada cop que un node fa un canvi, com un canvi al temps de vida.
- **Direcció IP d'origen (32 bits).**
- **Direcció IP destí (32 bits).**
- **Opcions i padding (bits variables):** El padding s'encarrega que la mida de la capçalera tingui una mida mínim, múltiple de 32 bits.

Exercici 2:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	162.159.135.234	192.168.1.108	TLSv1.2	137	Application Data
2	0.050425	192.168.1.108	162.159.135.234	TCP	54	52062 → 443 [ACK] Seq=1 Ack=84 Win=513 Len=0
14	1.953882	192.168.1.108	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
16	3.103948	192.168.1.108	192.168.1.1	DNS	87	Standard query 0x9731 AAAA time-A.timefreq.blrdoc.gov
18	3.163366	192.168.1.1	192.168.1.108	DNS	161	Standard query response 0x9731 AAAA time-A.timefreq.blrdoc.gov CNAME tim...
19	3.170873	192.168.1.108	132.163.96.1	TCP	66	53003 → 13 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
20	3.309779	132.163.96.1	192.168.1.108	TCP	66	13 → 53003 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 WS=64 SACK_PER...
21	3.310056	192.168.1.108	132.163.96.1	TCP	54	53003 → 13 [ACK] Seq=1 Ack=1 Win=131840 Len=0
22	3.446648	132.163.96.1	192.168.1.108	DAYTIME	105	DAYTIME Response
23	3.446648	132.163.96.1	192.168.1.108	TCP	54	13 → 53003 [FIN, ACK] Seq=52 Ack=1 Win=66688 Len=0
24	3.446774	192.168.1.108	132.163.96.1	TCP	54	53003 → 13 [ACK] Seq=1 Ack=53 Win=131840 Len=0
25	3.464168	192.168.1.108	132.163.96.1	TCP	54	53003 → 13 [FIN, ACK] Seq=1 Ack=53 Win=131840 Len=0
26	3.599865	132.163.96.1	192.168.1.108	TCP	54	13 → 53003 [ACK] Seq=53 Ack=2 Win=295168 Len=0
27	5.290491	162.159.135.234	192.168.1.108	TLSv1.2	133	Application Data
28	5.341779	162.159.135.234	192.168.1.108	TCP	54	52062 → 443 [ACK] Seq=1 Ack=163 Win=513 Len=0

1. Un cop determinada la IP, a quin port ens estem connectant? Quin protocol de transport fem servir?

La IP és **132.163.96.1**. Ens estem connectant al port **13**. Utilitzem el protocol TCP.

2. Identifica l'intercanvi de comunicacions que es produeix a nivell de DNS.

- **Quin protocol de transport fa servir DNS? Perquè?**

La funció del DNS és establir una adreça IP mitjançant el nom del domini. Utilitza protocol UDP (User Datagram Protocol). S'utilitza el protocol UDP en lloc del TCP quan ens interessa la velocitat més que la fiabilitat del paquet. En aquest cas és més important establir connexió amb el servidor DNS el més ràpid possible i que aquest no es sobrecarregui de peticions, per tant, s'utilitza aquest protocol per l'estalvi de temps.

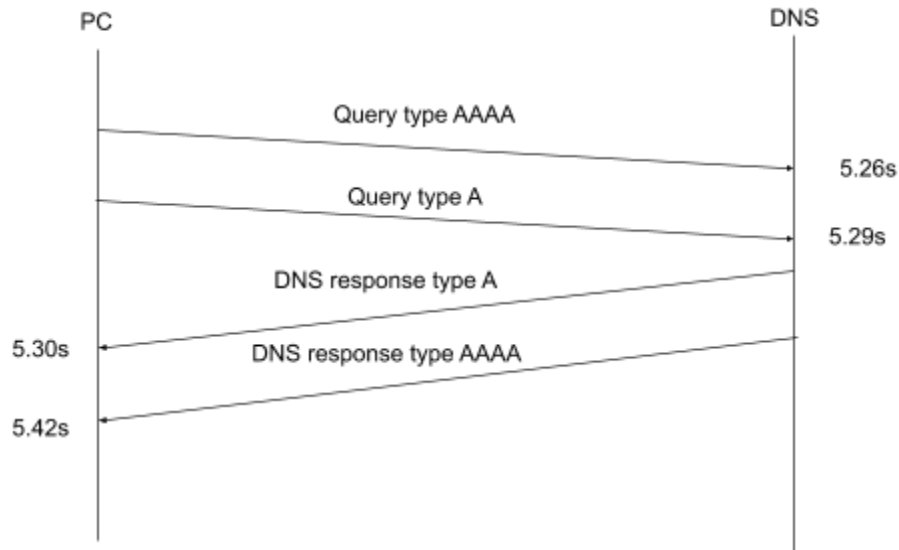
- **Quina és la IP del servidor de DNS?**

Podem veure que la IP del servidor DNS és la nostra IP, però en aquest cas utilitza el port 53 per connectar-se al servidor.

- **Com s'especifica la resposta? Què respon?**

La resposta que obtenim és una adreça IP. Respon a 132.163.96.1 que és la IP del domini a la qual ens volem connectar

- **Feu el diagrama temporal descrivint detalladament l'intercanvi d'informació entre el vostre ordinador i el servidor de DNS.**

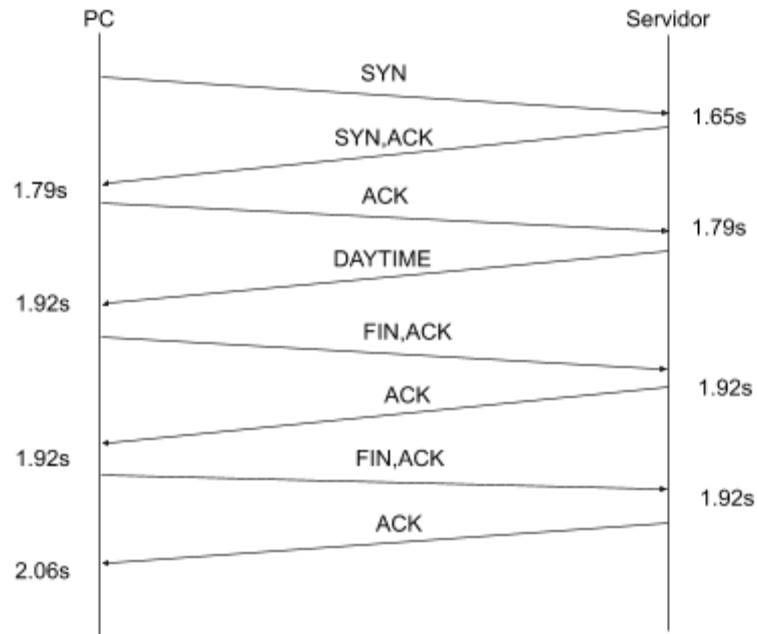


Troblem 2 tipus diferents de query, el tipus A demana la IPv4 mentre que el AAAA demana el IPv6. En el cas del query al servidor DNS ens retorna la direcció IPv4 132.163.96.1, en fer el query indiquem el domini d'on volem obtenir la informació, per fer una transmissió més ràpida utilitzem el protocol UDP, el servidor DNS busca la IP que volem a la seva taula d'adreces i ens l'envia de retorn amb el protocol UDP.

- **Un cop coneguda la IP destí, proporcionada pel servidor de DNS, identifica l'intercanvi de control que es produeix a nivell de TCP per la transmissió de la informació.**

Expliqueu que fa cada paquet i feu un diagrama temporal on es representa aquest intercanvi. Pren molta rellevància la utilització dels flags a TCP. Indiqueu que fan i com es fan servir per gestionar la comunicació.

No.	Time	Source	Destination	Protocol	Length	Info
387	1.655217	192.168.1.108	132.163.96.1	TCP	66	58757 → 13 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
419	1.792198	132.163.96.1	192.168.1.108	TCP	66	13 → 58757 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 WS=64 SACK_PERM=1
420	1.792312	192.168.1.108	132.163.96.1	TCP	54	58757 → 13 [ACK] Seq=1 Ack=1 Win=131840 Len=0
454	1.927493	132.163.96.1	192.168.1.108	DAYTIME	105	DAYTIME Response
456	1.928558	132.163.96.1	192.168.1.108	TCP	54	13 → 58757 [FIN, ACK] Seq=52 Ack=1 Win=66688 Len=0
457	1.928620	192.168.1.108	132.163.96.1	TCP	54	58757 → 13 [ACK] Seq=1 Ack=53 Win=131840 Len=0
458	1.929243	192.168.1.108	132.163.96.1	TCP	54	58757 → 13 [FIN, ACK] Seq=1 Ack=53 Win=131840 Len=0
516	2.068080	132.163.96.1	192.168.1.108	TCP	54	13 → 58757 [ACK] Seq=53 Ack=2 Win=295168 Len=0



Configurem el protocol TCP al port 58757 i comença enviant el paquet SYN (aquest és un bit de control dins del segment TCP, s'utilitza per sincronitzar els números de seqüència inicials d'una connexió del 3 way handshake). El servidor respon amb el paquet SYN,ACK i comunica que la connexió és correcta. Enviem el paquet ACK (indica que estem llest per iniciar la transmissió). El servidor ens envia el DAYTIME i ens envia les dades de la data i hora. Com ja hem rebut les dades comuniquem amb el paquet FIN,ACK que iniciem el fi de la transmissió. El servidor ens indica la finalització posant el flag FIN = 1. Es continua fent el procés de finalització fins que la transmissió es tanca.

Exercici 3:

1. Captureu el transit de la comunicació i desglosseu la comunicació en sí.

Després de fer la comanda 'ping www.google.com' al terminal de Windows capturem el següent:

No.	Time	Source	Destination	Protocol	Length	Info
31	0.917445	fe80::84b4:870e:7abc:...	fe80::5edc:96ff:fecc:cc11	DNS	94	Standard query 0x059f A www.google.com
32	0.936589	fe80::5edc:96ff:fecc:...	fe80::84b4:870e:7abc:9b5c	DNS	110	Standard query response 0x059f A www.google.com A 216.58.215.132
33	0.955135	192.168.1.108	216.58.215.132	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 34)
34	0.971589	216.58.215.132	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=112 (request in 33)
35	1.958236	192.168.1.108	216.58.215.132	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 36)
36	1.975218	216.58.215.132	192.168.1.108	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=112 (request in 35)

- **Expliqueu detalladament la captura, tal i com s'ha fet en l'exercici anterior**

En la captura, podem veure que primer utilitza DNS per demanar la adreça IP del domini Google. En aquest cas només fa un query de tipus A, ja que hem especificat explícitament fer el ping amb IPv4 (ja que si no ens mostrava el resultat en IPv6). Després utilitza el protocol ICMP per fer el ping entre el host i el servidor.

- **Què és el protocol ICMP?**

El protocol ICMP és utilitzat per informar de l'estat i situacions d'error. No se sol utilitzar com a intercanvi d'informació entre sistemes com ho fan les capes de transport, a excepció del ping i traceroute que utilitza el protocol ICMP per fins de diagnòstic.

- **Com funciona aquest protocol? Quins identificadors i flags fa servir?**

El protocol ICMP conté les següents parts:

- Type (8 bits): Si el type mostra un 8 significa que és una petició. Si mostra 0, seria una resposta.
- Codi (8 bits): Indica de quin tipus de ICMP és.
- Checksum: Dades de comprovació d'errors.
- Identificadors (BE, LE). Bits per comprovar la resposta esperada
- Número de seqüència (BE, LE). Serveixen per identificar que es la resposta esperada
- Data (32 bytes).

- Obriu el navegador i poseu `http://ip_obtinguda` a través del ping. S'obre la pàgina? Que captura el sniffer? Feu una explicació detallada.

La IP obtinguda és: 216.58.215.132. S'obre la pàgina principal de Google. El sniffer captura la comunicació entre el host i el servidor de Google que utilitzen els protocols TCP. Com que la IP la sabem i la posem directament al navegador en lloc del nom del domini, el DNS no ha d'intervenir en cap moment.

No.	Time	Source	Destination	Protocol	Length	Info
171	20.971211	192.168.1.108	216.58.201.168	TCP	66	57611 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146
172	20.971747	192.168.1.108	216.58.201.168	TCP	66	57612 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146
174	20.988517	216.58.201.168	192.168.1.108	TCP	66	80 → 57611 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
175	20.988517	216.58.201.168	192.168.1.108	TCP	66	80 → 57612 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
176	20.988686	192.168.1.108	216.58.201.168	TCP	54	57611 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
177	20.988767	192.168.1.108	216.58.201.168	TCP	54	57612 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
255	21.703532	192.168.1.108	216.58.201.168	TCP	54	57612 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131840 Len=0
256	21.704223	192.168.1.108	216.58.201.168	TCP	54	57611 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131840 Len=0
257	21.718203	216.58.201.168	192.168.1.108	TCP	54	80 → 57612 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0
258	21.718203	216.58.201.168	192.168.1.108	TCP	54	80 → 57611 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0
259	21.718311	192.168.1.108	216.58.201.168	TCP	54	57612 → 80 [ACK] Seq=2 Ack=2 Win=131840 Len=0
260	21.718421	192.168.1.108	216.58.201.168	TCP	54	57611 → 80 [ACK] Seq=2 Ack=2 Win=131840 Len=0
533	29.412302	192.168.1.108	216.58.201.168	TCP	66	57617 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146
534	29.412663	192.168.1.108	216.58.201.168	TCP	66	57618 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=146
537	29.440796	216.58.201.168	192.168.1.108	TCP	66	80 → 57617 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
538	29.440796	216.58.201.168	192.168.1.108	TCP	66	80 → 57618 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
539	29.440957	192.168.1.108	216.58.201.168	TCP	54	57617 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
540	29.441032	192.168.1.108	216.58.201.168	TCP	54	57618 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
551	31.710302	192.168.1.108	216.58.201.168	TCP	54	57618 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131840 Len=0
552	31.710605	192.168.1.108	216.58.201.168	TCP	54	57617 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131840 Len=0
557	31.726003	216.58.201.168	192.168.1.108	TCP	54	80 → 57618 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0
558	31.726133	192.168.1.108	216.58.201.168	TCP	54	57618 → 80 [ACK] Seq=2 Ack=2 Win=131840 Len=0

- Desglosseu la captura per connectar amb la web. Aneu al protocol TCP. Quin port de sortida heu fet servir? Identifiqueu algun protocol de control de flux? Expliqueu detalladament el que heu capturat.

S'ha utilitzat el port 80 per connectar amb el servidor DNS. El protocol TCP utilitza les flags per controlar el flux, com podem veure en la imatge d'amunt utilitza les flags: [SYN], [ACK] o [FIN].

La flag [SYN] sincronitza els números de la seqüència inicials.

La flag [ACK] és per confirmació

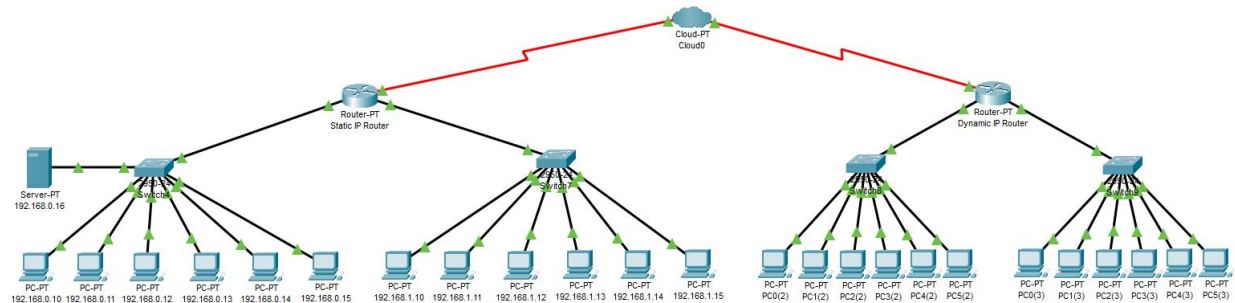
La flag [FIN] significa que és l'últim paquet.

Com a exemple, les dues primeres 'línies' activen la Flag SYN. Les dues següents activen la flag SYN i al mateix temps responen amb la Flag ACK com a confirmació a les dues primeres. Finalment les dues línies següents responen a les dues anteriors amb la flag ACK.

Exercici 4:

Muntem les dues xarxes que es demanen connectades a un servidor cloud.

La xarxa de l'esquerra correspon a la subnetting variable amb IP estàtiques, mentre que l'altra xarxa té un servidor DHCP per assignar les IP de forma dinàmica.



IP estàtiques:

Per configurar la xarxa de IP estàtiques hem hagut d'anar assignant manualment ordinador a ordinador les IP a utilitzar.

IP dinàmiques:

Per això hem hagut de configurar el servidor DHCP del router de la següent forma:

1. Ip dhcp excluded-address <<IP's>> # IP reservades per a dispositius específics
2. Ip dhcp pool <<NOM>> # Entrem en mode configuració d'un nou servidor DHCP
3. Default-router <<IP>> # Identifiquem el router
4. Dns-server <<IP>> # Definim el servidor DNS
5. Exit # Sortim del mode configuració

Habilitem les xarxes WAN:

Xarxa Estàtica	Xarxa Dinàmica
<p>Serial2/0</p> <p>Port Status <input checked="" type="checkbox"/> On</p> <p>Duplex <input type="radio"/> Full Duplex</p> <p>Clock Rate 2000000</p> <p>IP Configuration</p> <p>IPv4 Address 10.0.0.1</p> <p>Subnet Mask 255.0.0.0</p> <p>Tx Ring Limit 10</p>	<p>Serial2/0</p> <p>Port Status <input checked="" type="checkbox"/> On</p> <p>Duplex <input type="radio"/> Full Duplex</p> <p>Clock Rate 2000000</p> <p>IP Configuration</p> <p>IPv4 Address 10.0.0.2</p> <p>Subnet Mask 255.0.0.0</p> <p>Tx Ring Limit 10</p>

Configurem la NAT:

Per tal de transformar les IP en públiques per així poder tenir una identificació global i poder navegar per internet, configurarem la NAT en ambdós routers de forma dinàmica.

1. access-list <<N>> permit <<IP>> <<Màscara> # Traduïm les IP al rang especificat
2. Ip nat pool <<NOM>> <<IP1>> <<IP2>> netmask <<Màscara>> # Definim una piscina de IP a utilitzar del rang IP1 a IP2 amb la màscara especificada.
3. Ip nat inside source list <<N>> pool <<NAME>> especifiquem la piscina de IP a utilitzar dins de la nat interna.
4. Interface <<interfície local>>
5. Ip nat inside # Especifiquem la nat interna
6. Exit
7. Interface <<interfície wan>>
8. Ip nat outside # Especifiquem la nat externa
9. Exit
10. Ip route 0.0.0.0 0.0.0.0 s2/0 # Enrutem les IP de sortida

Comprovem el funcionament de la red fent PING entre les 2 xarxes:

```
C:\>
C:\>ping 172.16.0.12

Pinging 172.16.0.12 with 32 bytes of data:

Reply from 172.16.0.12: bytes=32 time=2ms TTL=126
Request timed out.
Reply from 172.16.0.12: bytes=32 time=2ms TTL=126
Request timed out.

Ping statistics for 172.16.0.12:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>

IPv4 Address.....: 172.16.0.12
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                  172.16.0.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
                  0.0.0.0

C:\>
```

3.029	--	192.168.1.13	ICMP
3.030	Switch7	192.168.1.11	STP
3.030	Switch7	192.168.1.10	STP
3.030	Switch7	192.168.1.12	STP
3.030	Switch7	192.168.1.13	STP
3.030	Switch7	Static IP Router	STP
3.030	Switch7	192.168.1.14	STP
3.030	Switch7	192.168.1.15	STP
3.030	192.168.1.13	Switch7	ICMP
3.031	Switch7	Static IP Router	ICMP
3.032	Static IP Router	Cloud0	ICMP
3.033	Cloud0	Dynamic IP R...	ICMP
3.034	Dynamic IP Ro...	Switch8	ICMP
3.035	Switch8	PC3(2)	ICMP
3.036	PC3(2)	Switch8	ICMP
3.037	Switch8	Dynamic IP R...	ICMP
3.038	Dynamic IP Ro...	Cloud0	ICMP
3.039	Cloud0	Static IP Router	ICMP
3.040	Static IP Router	Switch7	ICMP
3.041	Switch7	192.168.1.13	ICMP

Comprovem que s'està traduint les IP correctament:

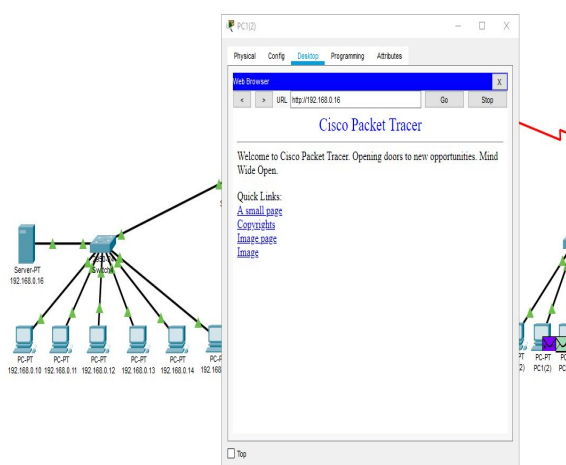
```
Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside
-----
icmp 161.116.96.2:18    192.168.1.12:18    161.116.97.5:18
161.116.97.5:18
icmp 161.116.96.2:19    192.168.1.12:19    161.116.97.5:19
161.116.97.5:19
icmp 161.116.96.2:20    192.168.1.12:20    161.116.97.12:20
161.116.97.12:20
icmp 161.116.96.2:21    192.168.1.12:21    161.116.97.12:21
161.116.97.12:21
icmp 161.116.96.2:22    192.168.1.12:22    161.116.97.12:22
161.116.97.12:22
icmp 161.116.96.2:23    192.168.1.12:23    161.116.97.12:23
161.116.97.12:23
icmp 161.116.96.2:24    192.168.1.12:24    161.116.97.12:24
161.116.97.12:24
```













Configurem el servidor web:

Bàsicament fiquem el servidor a la xarxa estàtica, definim el Default Gateway i introduïm la seva IP manualment, posteriorment iniciem els serveis d'http i https i fiquem un index.html al servidor que farà de pàgina principal.

Iniciem una connexió a aquest des d'un dels ordinadors de la xarxa dinàmica:

0.000	--	PC1(2)	TCP
0.001	PC1(2)	Switch8	TCP
0.002	Switch8	Router1	TCP
0.003	Router1	Cloud0	TCP
0.004	Cloud0	Static IP Router	TCP
0.005	Static IP Router	Switch4	TCP
0.006	Switch4	192.168.0.16	TCP
0.007	192.168.0.16	Switch4	TCP
0.008	Switch4	Static IP Router	TCP
0.009	Static IP Router	Cloud0	TCP
0.010	Cloud0	Router1	TCP
0.011	Router1	Switch8	TCP
0.012	Switch8	PC1(2)	TCP
0.012	--	PC1(2)	HTTP
0.013	PC1(2)	Switch8	TCP
0.013	--	PC1(2)	HTTP
0.014	PC1(2)	Switch8	HTTP
0.014	Switch8	Router1	TCP
0.015	Switch8	Router1	HTTP
0.015	Router1	Cloud0	TCP
0.016	Router1	Cloud0	HTTP
0.016	Cloud0	Static IP Router	TCP
0.017	Cloud0	Static IP Router	HTTP
0.017	Static IP Router	Switch4	TCP



0.018	Static IP Router	Switch4		HTTP
0.018	Switch4	192.168.0.16		TCP
0.019	Switch4	192.168.0.16		HTTP
0.020	192.168.0.16	Switch4		HTTP
0.021	Switch4	Static IP Router		HTTP
0.022	Static IP Router	Cloud0		HTTP
0.023	Cloud0	Router1		HTTP
0.024	Router1	Switch8		HTTP
 0.025	Switch8	PC1(2)		HTTP
 0.025	--	PC1(2)		TCP

Podem observar com establim connexió al servidor web correctament i els diferents empaquetaments que es realitzen.

Conclusions:

En aquesta pràctica hem adquirit diversos coneixements, entre ells com s'encapsulen els paquets de dades o com funcionen diferents protocols de TCP/IP, com el TCP, DNS, ICMP...

Amb el Packet Tracer hem après com configurar una NAT, així com un servidor web i hem aconseguit visualitzar la web connectant a través del port específic.