



**Universidad
Politécnica
de Cartagena**

**Escuela Técnica Superior de Ingeniería
de Telecomunicación**

**INSTRUMENTACIÓN TELEMÁTICA Y
LABORATORIO DE REDES**
3º Grado Ingeniería Telemática

Práctica 2-Sesión 2
**Routing de 2 redes LAN con conexión
a Internet con NAT**
(Revisión 2019-20)

EQUIPO 3

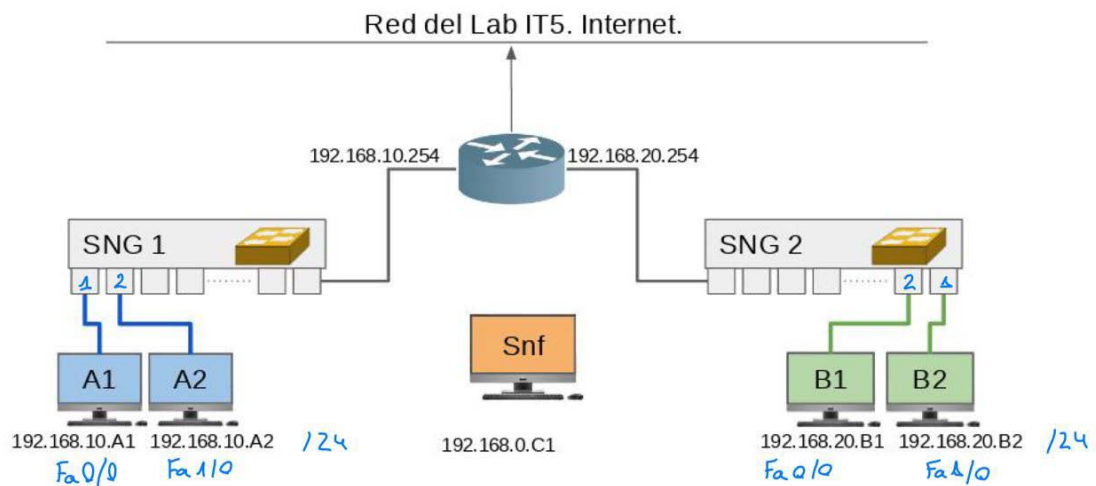
Profesores:
Alejandro Martínez Sala
Juan Carlos Sánchez Aarnoutse

CUESTIÓN 1: Esquema con la topología física y lógica objetivo de la maqueta.

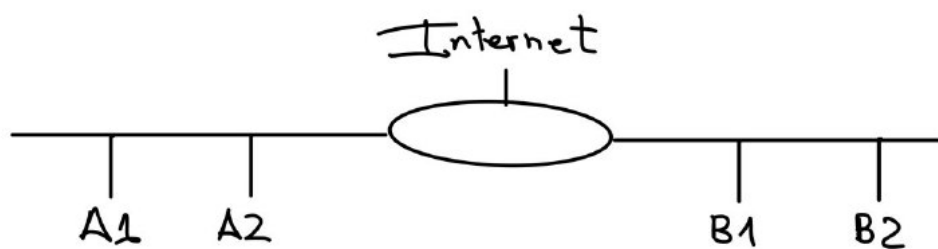
Haced vuestro propios esquemas con los “**planos objetivos**” (lo que se quiere lograr) de la maqueta.

En la topología física, indicad el código de la tarjeta Ethernet usada, el código de la electrónica de red (SNG1, SNG2, Router) y el nº de puerto usado en el cableado.

- Física:



- Lógica:



CUESTIÓN 2: Tablas de encaminamiento.

Representad las **tablas de encaminamiento** de los dispositivos IP según los requisitos de diseño del enunciado. Usad el siguiente formato:

PC 1

C/S	IP red	Máscara	Gateway	Interfaz
C	192.168.10.0	/24	-	Fa0/0
S	0.0.0.0	/0	192.168.10.254	Fa0/0

PC 2

C/S	IP red	Máscara	Gateway	Interfaz
C	192.168.10.0	/24	-	Fa0/0
S	0.0.0.0	/0	192.168.10.254	Fa0/0

PC 3

C/S	IP red	Máscara	Gateway	Interfaz
C	192.168.20.0	/24	-	Fa0/0
S	0.0.0.0	/0	192.168.20.254	Fa0/0

PC 4

C/S	IP red	Máscara	Gateway	Interfaz
C	192.168.20.0	/24	-	Fa0/0
S	0.0.0.0	/0	192.168.20.254	Fa0/0

CUESTIÓN 4: Cableado de la maqueta.

- a)
b) Usad el comando de Linux **ethtool**¹ para comprobar si el enlace está activo o no. Anotad las direcciones MAC de las tarjetas Ethernet.

```
ethtool eth0
```

RedB

Eth0: 00.E0.4C.68.0F.4D | Eth1(VM): 08.00.27.04.D0.63

RedA

Eth0: 00.E0.4C.68.91.44 | Eth1(VM): 08.00.27.D6.37.B5

Probad a quitar el cable de A1 y ejecutar de nuevo ethtool sobre eth0. ¿Hay alguna diferencia?

Sí, nos dice que el link no está detectado.

¹ Hay que tener en cuenta que las máquinas virtuales muestran una tarjeta de red virtualizada por lo que los parámetros mostrados no son reales. Por ese motivo se empleará **ethtool** sólo sobre las tarjetas físicas reales, en este caso A1 (eth0) y B1 (eth0). Para las máquinas virtuales habría que consultar eth1 del anfitrión, por ejemplo, en PCA ethtool eth1.

Con el cable A1 conectado

```
alumno@IT5-pc07:~$ ethtool eth0
Settings for eth0:
    Supported ports: [ TP MII ]
    Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Half 1000baseT/Full
    Supported pause frame use: No
    Supports auto-negotiation: Yes
    Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Half 1000baseT/Full
    Advertised pause frame use: Symmetric Receive-only
    Advertised auto-negotiation: Yes
    Link partner advertised link modes:  10baseT/Half 10baseT/Full
                                         100baseT/Half 100baseT/Full
                                         1000baseT/Full
    Link partner advertised pause frame use: Symmetric
    Link partner advertised auto-negotiation: Yes
    Speed: 1000Mb/s
    Duplex: Full
    Port: MII
    PHYAD: 0
    Transceiver: internal
    Auto-negotiation: on
Cannot get wake-on-lan settings: Operation not permitted
    Current message level: 0x00000033 (51)
                           drv probe ifdown ifup
    Link detected: yes
```

Con el cable A1 desconectado

```
alumno@IT5-pc07:~$ ethtool eth0
Settings for eth0:
    Supported ports: [ TP MII ]
    Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Half 1000baseT/Full
    Supported pause frame use: No
    Supports auto-negotiation: Yes
    Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Half 1000baseT/Full
    Advertised pause frame use: Symmetric Receive-only
    Advertised auto-negotiation: Yes
    Speed: 10Mb/s
    Duplex: Half
    Port: MII
    PHYAD: 0
    Transceiver: internal
    Auto-negotiation: on
Cannot get wake-on-lan settings: Operation not permitted
    Current message level: 0x00000033 (51)
                           drv probe ifdown ifup
    Link detected: no
```

Las diferencias se encuentran en el modo de transmisión de datos y en la velocidad. Al estar conectado el cable a A1 se pueden enviar y recibir datos simultáneamente (Full Duplex) pues no hay dominio de colisión. Al desconectarlo la conexión iría por WI-FI, que usa un medio compartido para transmitir información, por lo que no puede enviar y recibir información simultáneamente (Half-Duplex) ya que podrían producirse colisiones.

Al usar Half-Duplex como modo de transmisión la velocidad disminuye pues se reparte entre la transmisión y la recepción de datos.

NOTA: si la tarjeta no está activa (no aparecerá en el listado cuando se ejecuta **ifconfig**), **ethtool** no dará la información correcta. Para activar una tarjeta de red, por ejemplo la eth0, teclead en un terminal

```
ifconfig eth0 up
```

Para desactivar se emplea el mismo comando pero cambiando *up* por *down*.

Es posible que requiera permisos de superusuario, en ese caso se puede ejecutar con el comando **sudo** delante (pedirá una **clave**, que es **ITS**).

```
sudo ifconfig eth0 up
```

- c) Desactivad la tarjeta de red de uno de los equipos, comprobad los datos devueltos por **ethtool**, y volved a activarla.

Es lo mismo que haber desconectado el cable de red. Cambia Supports Wake-On: pumbg.

Anotad cualquier incidencia.

- d) **Comprobación de los modos (half / full duplex) y velocidades (10/100/1000).** Todas las tarjetas Ethernet tienen la **Autonegociación activada**. Comprobad con **ethtool** y anotad la velocidad y modo de cada tarjeta Ethernet. Indicadlo en vuestro esquema de la topología física.

RedA

Eth0: Full/100

Eth1: Full/1000

RedB

Eth0: Full/1000

Eth1 (VM): Full/1000

- e) **(Tarea para casa)**-Razonad e indicad en la topología física los **dominios broadcast** y **dominios de colisión** existentes.

3 dominios broadcast (192.168.10.0, 192.168.20.0 y 192.168.5.0) y ningún dominio de colisión.

- f) **(Tarea para casa)**-Razonad e indicad en la topología física los **dominios broadcast** y **dominios de colisión** existentes de la topología de la sesión anterior.

2 dominios broadcast (192.168.10.0 y 192.168.20.0) y 1 dominio de colisión perteneciente a la red en la que se encuentra el hub (192.168.20.0).

CUESTIÓN 5: Comprobación de la conexión entre equipos de una misma red.

- a) Comprobad con un ping la conectividad entre los diferentes equipos de una misma red (A1 y A2 y B1 y B2).

Todo funciona correctamente y sin ningún tipo de incidencia.

Anotad cualquier incidencia (funciona/no funciona).

- b) Al igual que en la sesión anterior, en este punto aún no está configurado el router, por lo que entre equipos de redes diferentes no debería funcionar (A1 y B1 y viceversa). Comprobadlo.

No funciona al no estar configurado el router.

Anotad cualquier incidencia (funciona/no funciona).

CUESTIÓN 6: Configuración del router para interconectar las dos redes LAN.

Sólo rellenar si ha habido alguna incidencia.

Sin incidencias

Route add default gw 192.168.20.254

CUESTIÓN 7: Comprobación de la conexión entre equipos las dos redes LAN.

Anotad si ha funcionado o no la conexión ssh.

Anotad cualquier incidencia.

¿Habéis podido comprobar que ssh va cifrado con la captura de Wireshark?

A partir de la captura ¿Qué puertos se han empleado en la conexión ssh?

Sí, ha funcionado y sin incidencias. **Mirar captura wireshark.**

1	0.000000000	192.168.10.31	192.168.20.31	TCP	74	34482 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=612674 TSecr=0 WS=128
2	0.000269110	192.168.20.31	192.168.10.31	TCP	74	22 → 34482 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=614563 TSecr=612674 WS=128
3	0.000282095	192.168.10.31	192.168.20.31	TCP	66	34482 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=612674 TSecr=614563
4	0.000412241	192.168.10.31	192.168.20.31	SSHv2	107	Client: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.1)
5	0.000523154	192.168.20.31	192.168.10.31	TCP	66	22 → 34482 [ACK] Seq=1 Ack=42 Win=29056 Len=0 TSval=614563 TSecr=612674
6	0.003685448	192.168.20.31	192.168.10.31	SSHv2	107	Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.6)
7	0.003694544	192.168.10.31	192.168.20.31	TCP	66	34482 → 22 [ACK] Seq=42 Ack=42 Win=29312 Len=0 TSval=612675 TSecr=614564
8	0.003919299	192.168.10.31	192.168.20.31	SSHv2	1402	Client: Key Exchange Init
9	0.004343479	192.168.20.31	192.168.10.31	SSHv2	1042	Server: Key Exchange Init
10	0.042586379	192.168.10.31	192.168.20.31	TCP	66	34482 → 22 [ACK] Seq=1378 Ack=1018 Win=32128 Len=0 TSval=612685 TSecr=614564
11	0.042715774	192.168.20.31	192.168.10.31	TCP	66	22 → 34482 [ACK] Seq=1018 Ack=1378 Win=31872 Len=0 TSval=614573 TSecr=612675
12	0.042723916	192.168.10.31	192.168.20.31	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
13	0.046940594	192.168.20.31	192.168.10.31	SSHv2	430	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=84)
14	0.046946343	192.168.10.31	192.168.20.31	TCP	66	34482 → 22 [ACK] Seq=1426 Ack=1382 Win=34048 Len=0 TSval=612686 TSecr=614574
15	0.048939942	192.168.10.31	192.168.20.31	SSHv2	82	Client: New Keys
16	0.087691530	192.168.20.31	192.168.10.31	TCP	66	22 → 34482 [ACK] Seq=1382 Ack=1442 Win=31872 Len=0 TSval=614585 TSecr=612686
17	0.087697713	192.168.10.31	192.168.20.31	SSHv2	110	Client: Encrypted packet (len=44)
18	0.087828611	192.168.20.31	192.168.10.31	TCP	66	22 → 34482 [ACK] Seq=1382 Ack=1486 Win=31872 Len=0 TSval=614585 TSecr=612696
19	0.087846371	192.168.10.31	192.168.20.31	SSHv2	110	Server: Encrypted packet (len=44)
20	0.087863591	192.168.10.31	192.168.20.31	SSHv2	134	Client: Encrypted packet (len=68)
21	0.088316476	192.168.20.31	192.168.10.31	SSHv2	118	Server: Encrypted packet (len=52)
22	0.126573903	192.168.10.31	192.168.20.31	TCP	66	34482 → 22 [ACK] Seq=1554 Ack=1478 Win=34048 Len=0 TSval=612706 TSecr=614585
23	3.791485320	192.168.10.31	192.168.20.31	SSHv2	150	Client: Encrypted packet (len=84)
24	3.797633180	192.168.20.31	192.168.10.31	SSHv2	94	Server: Encrypted packet (len=28)
25	3.797642982	192.168.10.31	192.168.20.31	TCP	66	34482 → 22 [ACK] Seq=1638 Ack=1506 Win=34048 Len=0 TSval=613623 TSecr=615512
26	3.797683417	192.168.10.31	192.168.20.31	SSHv2	178	Client: Encrypted packet (len=112)
27	3.835675211	192.168.20.31	192.168.10.31	TCP	66	22 → 34482 [ACK] Seq=1506 Ack=1750 Win=31872 Len=0 TSval=615522 TSecr=613623
28	3.857423997	192.168.20.31	192.168.10.31	SSHv2	1006	Server: Encrypted packet (len=940)
29	3.894575480	192.168.10.31	192.168.20.31	TCP	66	34482 → 22 [ACK] Seq=1750 Ack=2446 Win=36992 Len=0 TSval=613648 TSecr=615527
30	3.894730617	192.168.20.31	192.168.10.31	SSHv2	110	Server: Encrypted packet (len=44)
31	3.894735949	192.168.10.31	192.168.20.31	TCP	66	34482 → 22 [ACK] Seq=1750 Ack=2490 Win=36992 Len=0 TSval=613648 TSecr=615536
32	3.894785455	192.168.10.31	192.168.20.31	SSHv2	518	Client: Encrypted packet (len=452)

[illegible]

Los puertos empleados han sido

Puerto cliente: 34482

a) Comprobar con ping que hay acceso a Internet. Probad un ping a www.upct.es y también a 8.8.8.8. ¿Funcionan los dos? ¿Por qué?

Anotad cualquier incidencia.

c) ¿Por qué no se carga la página web?

Anotad cualquier incidencia.

e) Ahora ya debería funcionar la consulta a DNS. Probad de nuevo a capturar con wireshark la consulta web a www.upct.es. ¿Qué protocolos aparecen involucrados

en la consulta? ¿Qué puertos se emplean? ¿Cuál es la MAC del servidor www.upct.es?

```
> Frame 112: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
▼ Ethernet II, Src: RealtekS_68:91:44 (00:e0:4c:68:91:44), Dst: Routerbo_8f:0f:80 (74:4d:28:8f:0f:80)
  > Destination: Routerbo_8f:0f:80 (74:4d:28:8f:0f:80)
  > Source: RealtekS_68:91:44 (00:e0:4c:68:91:44)
  Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.10.31, Dst: 8.8.8.8
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 57
  Identification: 0x98bb (39099)
  > Flags: 0x4000, Don't fragment
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0xc721 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.10.31
  Destination: 8.8.8.8
▼ User Datagram Protocol, Src Port: 38855, Dst Port: 53
  Source Port: 38855
  Destination Port: 53
  Length: 37
  Checksum: 0xa586 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 10]
  > [Timestamps]
▼ Domain Name System (query)
  Transaction ID: 0x000c
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    [Response In: 166]
```

Los protocolos involucrados son:

- El IPv4 encargado de la conexión a nivel de Red.
- El UDP encargado de la conexión a nivel de Transporte.
- El DNS encargado de la conexión a nivel de Aplicación.

Los puertos involucrados son

El puerto DNS: 53

El puerto cliente: 38855

La MAC del servidor www.upct.es : 74:4d:28:8f:0f:80

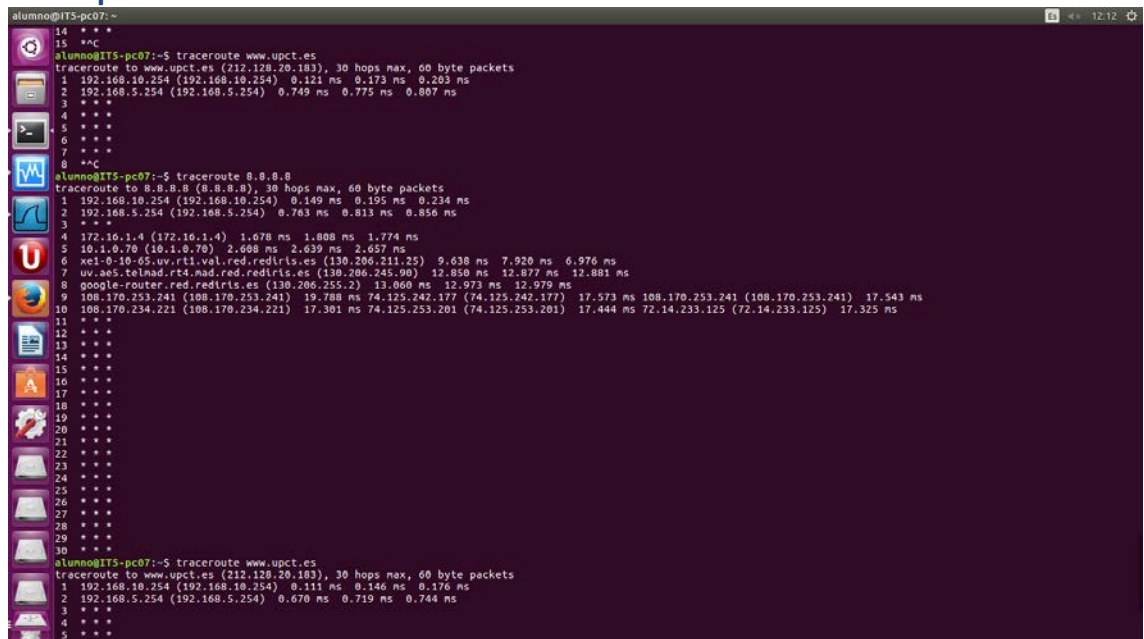
Responded a las cuestiones.

Anotad cualquier incidencia.

f) Nada que anotar.

- g) Probad ahora la herramienta traceroute para ver los saltos que hay en el camino hacia un equipo, por ejemplo el 8.8.8.8. y www.upct.es. ¿Hasta dónde llegan los paquetes?

Ver capturas.



```
alumno@ITS-pc07: ~$ traceroute www.upct.es
traceroute to www.upct.es (212.128.20.183), 30 hops max, 60 byte packets
 1 192.168.10.254 (192.168.10.254) 0.121 ms 0.173 ms 0.203 ms
 2 192.168.5.254 (192.168.5.254) 0.749 ms 0.775 ms 0.807 ms
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
alumno@ITS-pc07: ~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 192.168.10.254 (192.168.10.254) 0.149 ms 0.192 ms 0.234 ms
 2 192.168.5.254 (192.168.5.254) 0.761 ms 0.811 ms 0.856 ms
 3 * * *
 4 172.16.1.4 (172.16.1.4) 1.678 ms 1.808 ms 1.774 ms
 5 10.1.0.70 (10.1.0.70) 2.608 ms 2.639 ms 2.657 ms
 6 xel-0-10-65.uv.rti.val.red.rediris.es (130.206.211.25) 9.638 ms 7.920 ms 6.976 ms
 7 uv.aes.telmad.rt4.mad.red.rediris.es (130.206.245.90) 12.850 ms 12.877 ms 12.881 ms
 8 google-router.red.rediris.es (130.206.255.2) 11.060 ms 12.973 ms 12.979 ms
 9 108.170.253.241 (108.170.253.241) 19.788 ms 74.125.242.177 (74.125.242.177) 17.573 ms 108.170.253.241 (108.170.253.241) 17.543 ms
10 108.170.234.221 (108.170.234.221) 17.301 ms 74.125.253.201 (74.125.253.201) 17.444 ms 72.14.233.125 (72.14.233.125) 17.325 ms
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
alumno@ITS-pc07: ~$ traceroute www.upct.es
traceroute to www.upct.es (212.128.20.183), 30 hops max, 60 byte packets
 1 192.168.10.254 (192.168.10.254) 0.111 ms 0.146 ms 0.176 ms
 2 192.168.5.254 (192.168.5.254) 0.670 ms 0.719 ms 0.744 ms
 3 * * *
 4 * * *
 5 * * *
```

Si hacemos traceroute para www.upct.es vemos que llega hasta el router con dirección IP 192.168.5.254 en dos saltos.

Si hacemos traceroute para la dirección 8.8.8.8 llega hasta la dirección IP 108.170.234.221 en 10 saltos

Responded a las cuestiones.

Anotad cualquier incidencia.

CUESTIÓN 9: Captura de tráfico de NAT para ver cómo funciona.

Vamos a comprobar qué está sucediendo con NAT.....

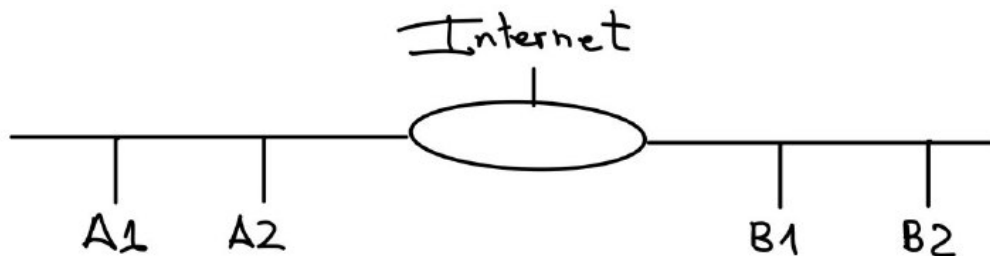
Arrancad una captura de tráfico en PCC, escuchando en las dos tarjetas en modo promiscuo. Una vez iniciada la captura, desde PCC lanzad un ping a la dirección 192.168.5.254. Observad la captura, sobre todo las direcciones IP de los paquetes y las MACs.

- ¿Son correctas o creéis que debería haber algo diferente? Explicad con los datos capturados cómo opera NAT en vuestro router.

Si son correctas, al enviar el paquete, cuando llega al router este cambiara la ip origen por la suya.

Práctica 2-Sesión 2: Routing con NAT y AP wifi – captura de tráfico
Instrumentación telemática y laboratorio de redes, 3º Grado Ingeniería Telemática

1	0.000000	192.168.5.254	255.255.255.255	UDP	215	55825 → 7437	Len=173
2	0.429788	Cisco_0e:63:96	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/0/00:10:b5:99:29:2b	Cost = 19 Port = 0x8016
3	2.445877	Cisco_0e:63:96	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/0/00:10:b5:99:29:2b	Cost = 19 Port = 0x8016
4	2.748617	Cisco_0e:63:96	Cisco_0e:63:96	LOOP	60	Reply	
5	3.024058	192.168.5.254	255.255.255.255	UDP	215	55825 → 7437	Len=173
6	3.106351	192.168.10.11	192.168.5.254	ICMP	98	Echo (ping) request	id=0x2dd9, seq=1/256, ttl=64 (reply in 8)
7	3.106602	192.168.5.100	192.168.5.254	ICMP	98	Echo (ping) request	id=0x2dd9, seq=1/256, ttl=63 (reply in 9)
8	3.107961	192.168.5.254	192.168.10.11	ICMP	98	Echo (ping) reply	id=0x2dd9, seq=1/256, ttl=63 (request in 6)
9	3.107915	192.168.5.254	192.168.5.100	ICMP	98	Echo (ping) reply	id=0x2dd9, seq=1/256, ttl=64 (request in 7)
10	3.197694	192.168.10.11	8.8.8.8	DNS	86	Standard query 0x6538 PTR 254.5.168.192.in-addr.arpa	
11	3.197891	192.168.5.100	8.8.8.8	DNS	86	Standard query 0x6538 PTR 254.5.168.192.in-addr.arpa	
12	3.197696	192.168.10.11	8.8.8.8	DNS	86	Standard query 0x1c21 PTR 11.10.168.192.in-addr.arpa	
13	3.211003	8.8.8.8	192.168.10.11	DNS	86	Standard query response 0x1c21 No such name PTR 11.10.168.192.in-addr.arpa	
14	3.197893	192.168.5.100	8.8.8.8	DNS	86	Standard query 0x1c21 PTR 11.10.168.192.in-addr.arpa	
15	3.210973	8.8.8.8	192.168.5.100	DNS	86	Standard query response 0x1c21 No such name PTR 11.10.168.192.in-addr.arpa	
16	3.211303	8.8.8.8	192.168.10.11	DNS	86	Standard query response 0x6538 No such name PTR 254.5.168.192.in-addr.arpa	
17	3.211097	8.8.8.8	192.168.5.100	DNS	86	Standard query response 0x6538 No such name PTR 254.5.168.192.in-addr.arpa	
18	4.108083	192.168.10.11	192.168.5.254	ICMP	98	Echo (ping) request	id=0x2dd9, seq=2/512, ttl=64 (reply in 20)
19	4.108293	192.168.5.100	192.168.5.254	ICMP	98	Echo (ping) request	id=0x2dd9, seq=2/512, ttl=63 (reply in 21)
20	4.112245	192.168.5.254	192.168.10.11	ICMP	98	Echo (ping) reply	id=0x2dd9, seq=2/512, ttl=63 (request in 18)
21	4.112252	192.168.5.254	192.168.5.100	ICMP	98	Echo (ping) reply	id=0x2dd9, seq=2/512, ttl=64 (request in 19)
22	4.546961	Cisco_0e:63:96	CDP/VTP/DTP/PagP/UD...	CDP	370	Device ID: Switch Port ID: FastEthernet0/20	
23	4.547915	Cisco_0e:63:96	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/0/00:10:b5:99:29:2b	Cost = 19 Port = 0x8016
24	5.109472	192.168.10.11	192.168.5.254	ICMP	98	Echo (ping) request	id=0x2dd9, seq=3/768, ttl=64 (reply in 26)
25	5.109689	192.168.5.100	192.168.5.254	ICMP	98	Echo (ping) request	id=0x2dd9, seq=3/768, ttl=63 (reply in 27)
26	5.111905	192.168.5.254	192.168.10.11	ICMP	98	Echo (ping) reply	id=0x2dd9, seq=3/768, ttl=63 (request in 24)
27	5.111915	192.168.5.254	192.168.5.100	ICMP	98	Echo (ping) reply	id=0x2dd9, seq=3/768, ttl=64 (request in 25)
28	6.048107	192.168.5.254	255.255.255.255	UDP	215	55825 → 7437	Len=173
29	6.111351	192.168.5.100	192.168.5.254	ICMP	98	Echo (ping) request	id=0x2dd9, seq=4/1024, ttl=63 (reply in 31)
30	6.111146	192.168.10.11	192.168.5.254	ICMP	98	Echo (ping) request	id=0x2dd9, seq=4/1024, ttl=64 (reply in 32)
31	6.111923	192.168.5.254	192.168.5.100	ICMP	98	Echo (ping) reply	id=0x2dd9, seq=4/1024, ttl=64 (request in 29)
32	6.111916	192.168.5.254	192.168.10.11	ICMP	98	Echo (ping) reply	id=0x2dd9, seq=4/1024, ttl=63 (request in 30)



Responded a las cuestiones.
Anotad cualquier incidencia.

CUESTIÓN 10: Algo más sobre DNS

Arrancad una captura de tráfico de nuevo en PCC.

Abrid un terminal en A1 y ejecutad `nslookup www.google.es` ¿Cuál es la IP del servidor de google? ¿Qué protocolo de transporte se usa? ¿Cuál es el puerto usado por el cliente dns y el servidor dns?

La IP del servidor de Google es 8.8.8.8. El protocolo de transporte que se usa es UDP. El puerto usado por el cliente es el puerto 52086, y el usado por el servidor dns es el puerto 53.

Responded a las cuestiones.

Anotad cualquier incidencia.