

Redes de Computadores

Entregable 2

Nombre: Alejandro Rodríguez López

Tabla de Contenido

Ejercicio 1 (4 puntos).....	3
NAT.....	4
Dispositivos y reparto de IPs.....	6
Ejercicio 2 (1 punto).....	7
Tamaño de la ventana.....	7
Algoritmo Reno.....	8
Ejercicio 3 (2,5 puntos).....	9
Filtros.....	10
IP/MAC.....	12
Conexiones TCP.....	12
Puerto petición web.....	12
PUSH.....	12
Ejercicio 4 (2,5 puntos).....	13
ARP.....	13
NTP.....	13
DHCP.....	14
DNS.....	14
SMTP/POP3/IMAP.....	14

Tabla de Figuras

Figure 1: Problema 1.....	3
Figure 2: NAT, 1.....	4
Figure 3: NAT, 2.....	4
Figure 4: NAT, 3.....	5
Figure 5: Solución Problema 1.....	6

Tabla de Algoritmos

Algoritmo NAT.....	5
Algoritmo Reno.....	8

Table de Capturas de pantalla

Screenshot 1: ping www.uva.es.....	12
Screenshot 2: ntpd -gq.....	13
Screenshot 3: dhcpcd -N eno1.....	14
Screenshot 4: ping www.alexrl.com.....	14
Screenshot 5: telnet smtp.gmail.com 587.....	14

Ejercicio 1 (4 puntos)

Un grupo de investigación de la universidad está montando su propio laboratorio dentro de la escuela y necesita diseñar el montaje de los equipos que lo compondrán. En dicho laboratorio hay 1 servidor que necesita poder acceder a equipos externos, además de tener acceso a ellos desde el exterior sin habilitar el reenvío de puertos. Se poseen también 5 PCs que necesitan poder comunicarse con el exterior, pero no es necesario que dispongan de una IP pública. Dichos PCs tienen que pertenecer los 5 a la misma subred, pudiendo el servidor formar parte de ella o de una red externa.

Tras hablar con el servicio informático nos comunican que podremos utilizar el rango de direcciones 172.20.16.184-172.20.16.191, además de que está libre la dirección 172.20.16.220, la cual tiene que utilizar obligatoriamente una máscara de 26 bits. La salida a Internet del laboratorio debe realizarse a través del *router* principal de la escuela, el cual posee la dirección 172.20.16.205/26. En la figura que aparece a continuación, se puede ver un esquema simplificado de toda la información obtenida:

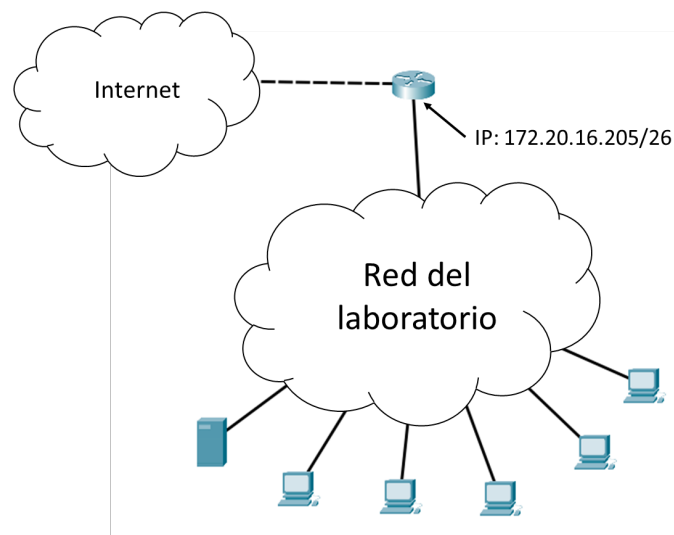


Figure 1: Problema 1.

Para resolver el problema anterior, será necesario utilizar como apoyo el rango de direcciones reservadas 10.0.0.192/26 y la técnica NAT (*Network Address Translation*) estudiados en la asignatura.

NAT

- a) ¿Cómo permite NAT ampliar el rango de direcciones posibles? Realiza una breve explicación con las diferentes alternativas que permite NAT para ampliar este rango. **(1 punto)**

El sistema NAT tiene como objetivo la reutilización de direcciones IP. Para ello, utilizará una dirección IP para reconocer sólo un router en lugar de cada equipo de una red.

En la ilustración siguiente se representan dos redes, una interna que se corresponde con una red cualsea y una externa que corresponde al resto de redes con las que es necesario cruzar la puerta de enlace para comunicarse.

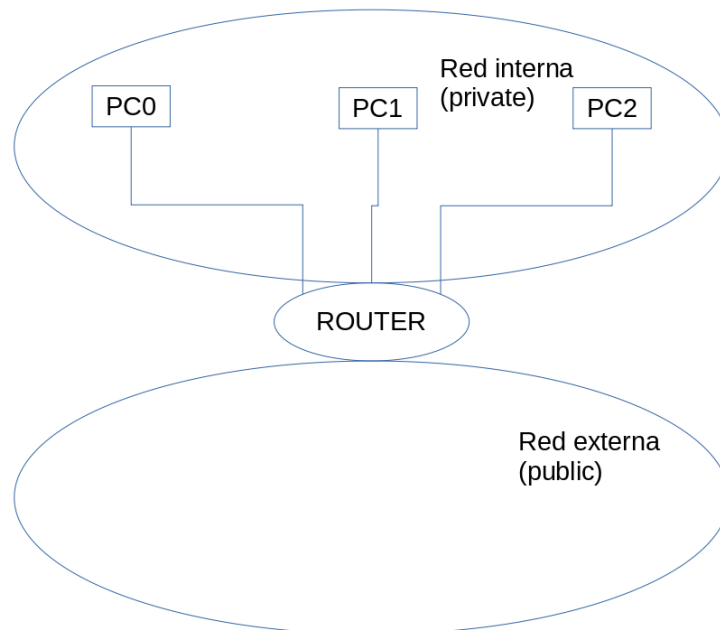


Figure 2: NAT, 1.

Si no se utilizase NAT, habría una dirección IP para cada equipo y para el router. Al utilizar NAT, sólo habrá una dirección IP para el router. Esto no significa que los equipos PCX no tengan direcciones IP, sí las tienen, pero esas direcciones IP también son asignadas a los equipos PCX de otras redes ajenas a la interna.

Para permitir que otra red tenga equipos con las mismas IPs, será necesario implementar una nueva funcionalidad en cada router. Deberán ser capaces de traducir direcciones, ya que en el ámbito de la red interna utilizaremos unas IPs para referirnos a los equipos y en ámbito externo nos referiremos a los de otras redes.

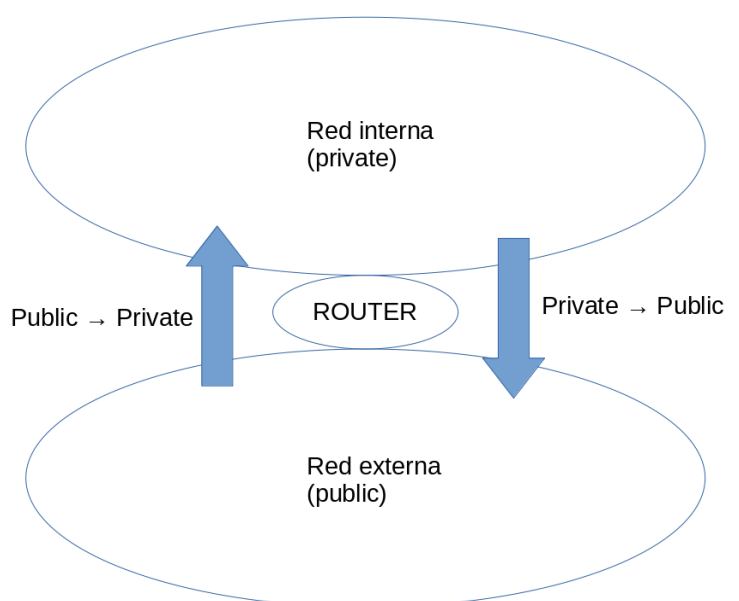


Figure 3: NAT, 2.

Supongamos la siguiente traza, en la que prestaremos particular atención a las direcciones de origen y destino:

Un equipo PC0 perteneciente a una red se comunica con otro equipo PC1 de otra red.

1. El mensaje que enviará PC0 tendrá como origen la IP de PC0 (Y.Y.Y.Y) y como destino aquella del PC1 (Z.Z.Z.Z).
2. Como PC1 no pertenece a la red de PC0, el mensaje se envía a la puerta de enlace (X.X.X.X).
3. El router recibe un mensaje Y.Y.Y.Y → Z.Z.Z.Z, como Z.Z.Z.Z es de otra red, sustituye Y.Y.Y.Y por X.X.X.X, anota que se está esperando una respuesta proveniente de Z.Z.Z.Z cuyo destino es Y.Y.Y.Y y envía el mensaje.
4. PC1 recibe un mensaje proveniente de X.X.X.X, envía su respuesta con origen Z.Z.Z.Z y destino X.X.X.X.
5. El router recibe un mensaje proveniente de Z.Z.Z.Z con destino X.X.X.X, el equipo Y.Y.Y.Y estaba a la espera de esta respuesta. El router la reenvía con destino Y.Y.Y.Y.
6. PC0 recibe la respuesta de origen Z.Z.Z.Z.

Simplemente, el único cambio que está realizando el router es:

- Para los paquetes que se envían: anotar direcciones y cambiar su dirección de origen
- Para los paquetes que se reciben: revisar direcciones de origen en el diccionario y cambiar su dirección de destino.

Algoritmo NAT

```
// Supuesto que esta clase extends LogicaRouterSinNAT

@Override
private void enviarPaquete (Paquete p) {
    if (! RED_INTERNA.contains(p.getDestino())) {
        this.listaEspera.put(p.getDestino(), p.getOrigen());
        p.setOrigen(this.IP);
    }
    super.enviarPaquete(p);
}

@Override
private void recibirPaquete (Paquete p) {
    if (this.listaEspera.containsKey(p.getOrigen())) {
        p.setDestino(listaEspera.get(p.getOrigen()));
        this.listaEspera.removeKey(p.getOrigen());
    }
    super.recibirPaquete(p);
}
```

Con este procedimiento, nos hemos comunicado con un equipo ajeno sin utilizar la IP del PC0 fuera de la red interna, si hubiese un PC2 en la red interna que también se quisiese comunicar con otra red, el mensaje también saldría con la IP del router.

Al aislar el uso de algunas direcciones IP en el ámbito interno, permitimos la posibilidad de que éstas se puedan repetir en todas las redes internas.

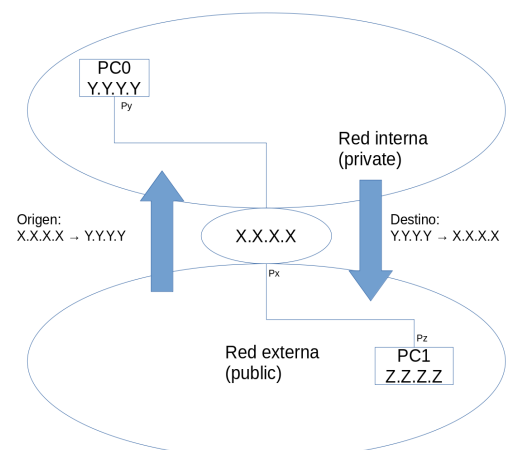


Figure 4: NAT, 3.

Dispositivos y reparto de IPs.

- b) ¿Qué equipos (*hubs*, *switchs* o *routers*) serán necesarios para poder realizar una configuración de red que permita cumplir todos los requisitos mencionados al principio del ejercicio? Explica por qué es necesario cada equipo extra a la hora de realizar la configuración y haz un esquema en el que se conecten todos los PCs y servidores a los equipos propuestos, además de asignar las direcciones IPs (utiliza NAT/PAT si es necesario) correspondientes a todas las interfaces utilizadas. **(3 puntos)**

Se buscará una configuración que cumpla las siguientes condiciones:

- La dirección del servidor es estática y conocida.
- Se utiliza NAT/PAT en alguna forma.
- Sólo se utilizan las IPs siguientes:
 - 172.20.16.184 a 172.20.16.191
 - 172.20.16.220
- La interfaz del router principal con la que se debe conectar la red del laboratorio tiene la ip 10.0.0.192/26
- El rango de IPs disponibles para NAT corresponde al de la subred 10.0.0.192/26

Dado que la dirección IP del servidor debe ser conocida, no puede estar afectada por NAT, mientras que los 5 equipos sí estarán afectados por NAT. Para hacer esta división, será necesario un router que separe al servidor de los equipos, para ello, el servidor se encontrará conectado a una interfaz del router y los 5 equipos a otra. Esto es, el servidor tendrá una subred y los 5 equipos otra.

Para poder conectar los 5 equipos en una única subred deberemos utilizar un switch para poder conectar los 5 a la misma interfaz del router.

Las direcciones IP de la subred del servidor serán estáticas en el rango [172.20.16.184, 172.20.16.191] mientras que las de la subred de los equipos serán NAT en 10.0.0.192/26.

Concretamente, las IP podrían ser las siguientes:

- | | |
|--|------------------------------|
| • Interfaz router principal: 172.20.16.205/26. | • IP equipo 1: 10.0.0.0.194. |
| • Interfaz router laboratorio: 172.20.16.220/26. | • IP equipo 2: 10.0.0.0.195. |
| • Interfaz router servidor: 172.20.16.184/29. | • IP equipo 3: 10.0.0.0.196. |
| • IP servidor: 172.20.16.185/29. | • IP equipo 4: 10.0.0.0.197. |
| • IP router equipos (NAT): 10.0.0.193. | • IP equipo 5: 10.0.0.0.198. |

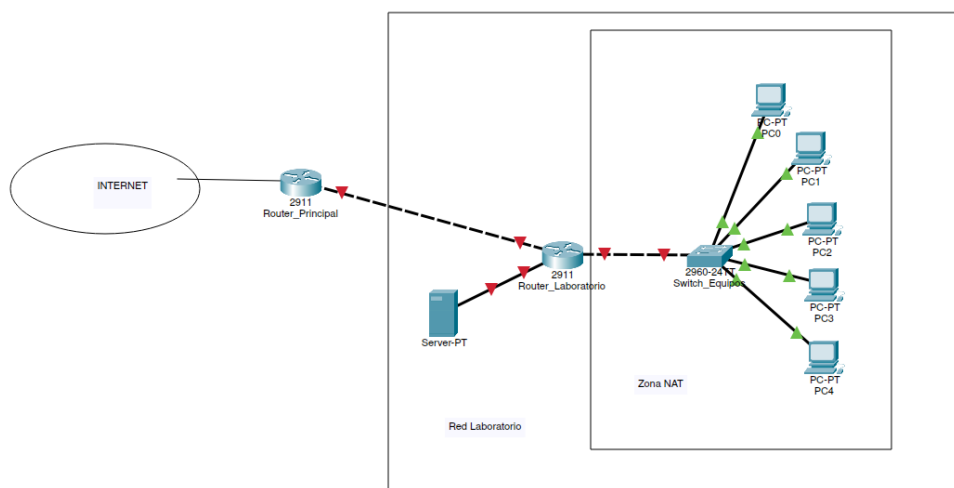


Figure 5: Solución Problema 1.

Ejercicio 2 (1 punto)

Tenemos un algoritmo de control de congestión TCP Reno, con un umbral de tamaño de ventana al inicio de 12. Tras el ciclo 8, se reciben 3 ACKs duplicados. Después del ciclo 14 salta un temporizador RTO para reenviar un paquete. Tras el ciclo 19, se reciben de forma consecutiva 2 ACKs repetidos. Por último, tras el ciclo 21, se vuelven a recibir 4 ACKs repetidos.

Dibuje hasta el ciclo 25, la gráfica asociada al tamaño de ventana, e indique cuáles son los diferentes umbrales cuando se produce una pérdida.

Nota: Puedes editar la gráfica inferior en Word con botón derecho -> modificar datos, o generar tu propia gráfica con un gestor de hojas de cálculo tipo Excel y pegar la gráfica aquí.

Respuesta:

Tamaño de la ventana



Algoritmo Reno

El algoritmo Reno se puede dividir en dos secciones: Antes del valor umbral y después del valor umbral.

Para los instantes donde el tamaño de ventana es inferior al umbral, el tamaño de ventana pasa a ser: 2^x , siendo x el instante.

Para los instantes donde el tamaño de ventana es superior o igual al umbral, el tamaño de ventana pasaría a ser $a \cdot x + t$, siendo a un valor positivo cualsea, x el instante y t el tamaño de ventana actual.

Cuando salta un temporizador RTO o se reciben un mínimo de 3 ACKs repetidos, tanto el umbral como el tamaño de ventana se reduce a la mitad del actual tamaño de ventana, de forma que el crecimiento para los siguientes intervalos siga siendo lineal.

Algoritmo Reno

```
private void instante (int x, ACK acks[], boolean RTO) {
    if (RTO || hayTresAckIgualesEn(acks)) {
        this.tamannoVentana /= 2;
        this.umbral = this.tamannoVentana;
        this.instanteUltimaCaida = x;
    } elif (this.tamannoVentana < this.umbral) {
        // Supuesto que el instante inicial es el x=0:
        this.tamannoVentana = Math.min(Math.pow(2, x), this.umbral);
    } else {
        this.tamannoVentana = this.umbral+this.A*(x - this.instanteUltimaCaida);
    }
}
```


Ejercicio 3 (2,5 puntos)

Utilizando Wireshark realiza una captura de cómo tu ordenador obtiene la página web de la Universidad de Valladolid (<https://www.uva.es/>). Para realizar esta captura es aconsejable tener cerradas todas las aplicaciones que puedan generar tráfico en segundo plano, además de utilizar un navegador diferente al que emplees habitualmente, para evitar que la página se cargue desde la memoria del ordenador en lugar de descargarse de Internet. Dicha captura deberá ser filtrada mediante los comandos adecuados y exportada mediante la instrucción *File/Export Specified Packets...* de tal forma que en ella únicamente quede el tráfico intercambiado entre el ordenador original y la web de la universidad en un archivo de formato *.pcap*. El resultado obtenido deberá ser subido a la entrega habilitada en el campus virtual con el nombre *UoXXXXXX_Captura_WUniv.pcap*. Además de la captura, será necesario contestar a las cuestiones que se plantean a continuación.

Nota: Si por razones de privacidad no se desea subir la captura *pcap* a la entrega del campus, las respuestas a todas las cuestiones deberán adjuntar capturas de pantalla con la información sensible tapada, pero donde se pueda observar claramente cómo se ha obtenido la respuesta.

Filtros

- a) La nota de esta cuestión se corresponde a la pregunta además de a la captura completa, ya sea en formato .pcap o subiendo una o varias capturas de pantalla con todos los paquetes ¿Qué filtro has empleado para aislar el tráfico entre la web de la universidad y tu PC? **(0.5 puntos)**

Desde un principio parecería que el filtro `ip.addr == <ip_universidad> [|| dns]` sería suficiente, sin embargo, sólo serviría si `<mi_ip>` fuese la única en comunicación con `<ip_universidad>`. Si hubiese un segundo equipo en contacto con www.uva.es, aparecerían también sus mensajes.

Deberemos asegurarnos de que el equipo al otro lado de la comunicación con `<ip_universidad>` es `<mi_ip>`.

Sean las siguientes condiciones:

A = La dirección IP de destino es la de la universidad (desconocida inicialmente).

B = La dirección IP de destino es la de mi sistema.

C = La dirección IP de origen es la de mi sistema.

D = La dirección IP de origen es la de la universidad (desconocida inicialmente).

E = El paquete es DNS.

La condición se podría comprender como:

“Si la dirección IP de destino es la de la universidad y la de origen es la mía o la de origen es la de la universidad y la de origen es la mía”. ($A \wedge B \vee C \wedge D$)

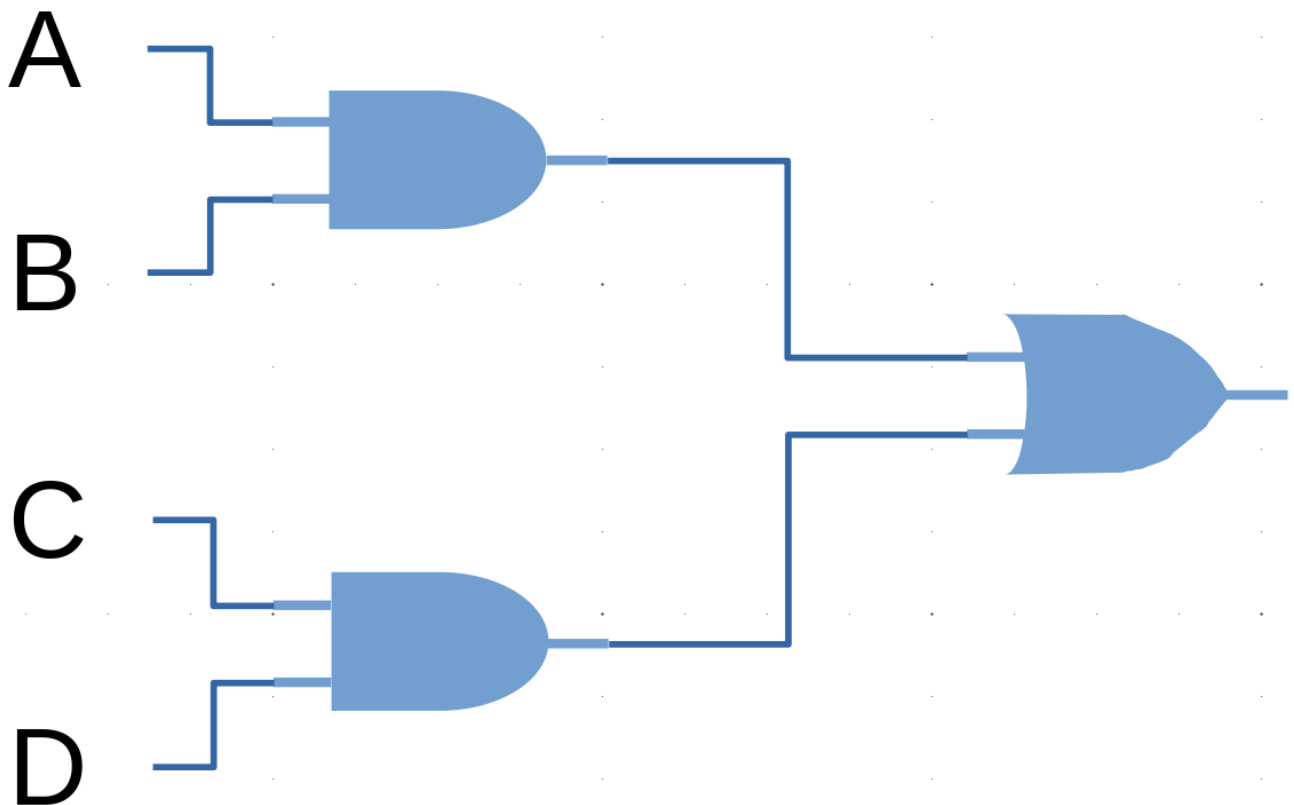


Illustration 1: Representación Lógica.

Sin embargo, esta condición bloquearía también las comunicaciones con el servidor DNS para resolver el nombre <https://www.uva.es/>, si quisiésemos añadir dichos paquetes de comunicación DNS, la condición sería:

“Si la dirección IP de destino es la de la universidad y la de origen es la mía o la de origen es la de la universidad y la de origen es la mía o el paquete es un DNS”. ($A \wedge B \vee C \wedge D \vee E$)

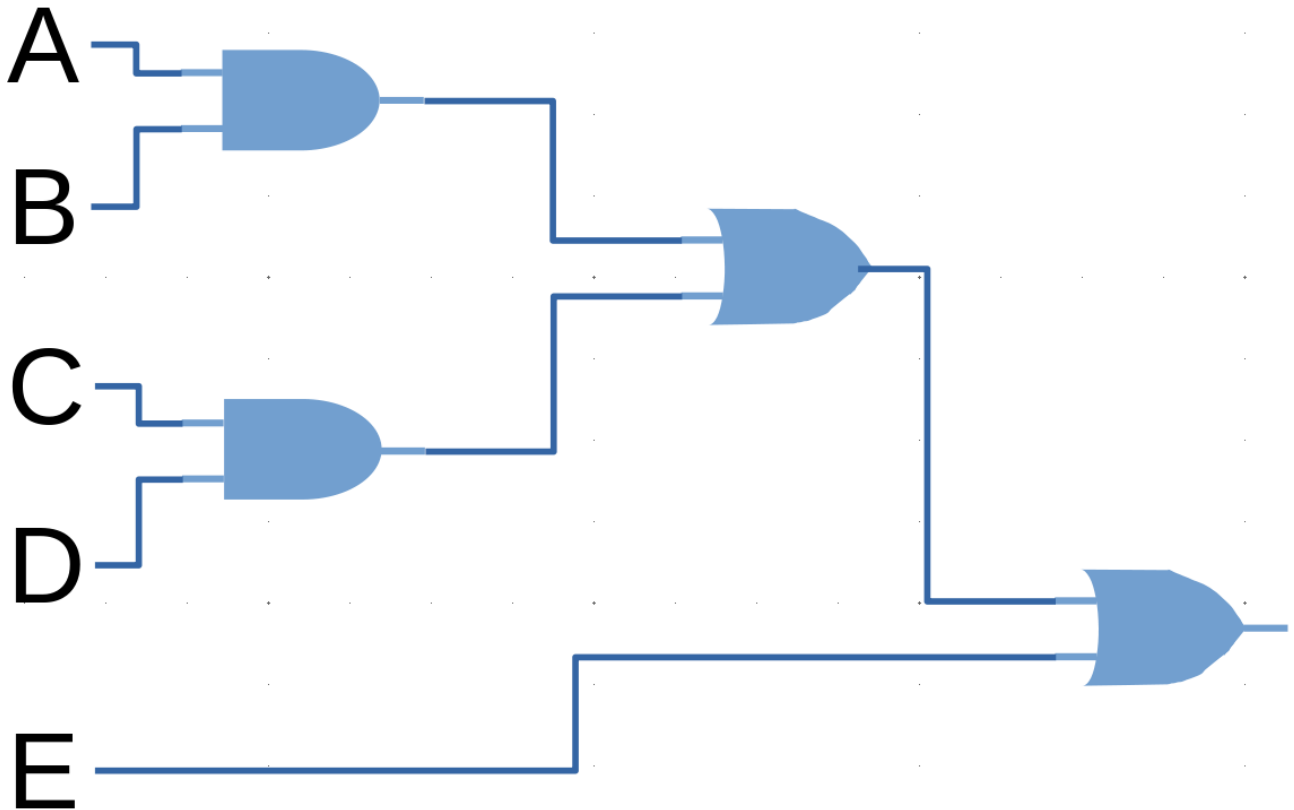


Illustration 2: Representación Lógica, con DNS.

Utilizando entonces la sintaxis de Wireshark, los filtros serían:

- `(ip.dst_host == <mi_ip> && ip.src_host == <ip_universidad>) || (ip.src_host == <mi_ip> && ip.dst_host == <ip_universidad>)`, para la versión sin DNS.
- `(ip.dst_host == <mi_ip> && ip.src_host == <ip_universidad>) || (ip.src_host == <mi_ip> && ip.dst_host == <ip_universidad>) || dns`, para la versión con DNS.

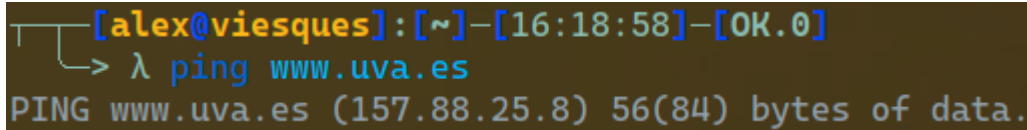
IP/MAC

- b) ¿Cuál es la dirección IP de la web de la universidad? ¿Y su dirección MAC? **(0.5 puntos)**

Para hallar la dirección IP de la universidad desde la captura de Wireshark, observamos la sección IP en cualquiera de los paquetes:

IP > Destination Address > 157.88.25.8

Alternativamente, se puede utilizar ping:



```
[alex@viesques]:[~]-[16:18:58]-[OK.0]
> λ ping www.uva.es
PING www.uva.es (157.88.25.8) 56(84) bytes of data.
```

Screenshot 1: ping www.uva.es

A pesar de que en el apartado Ethernet II de los paquetes se muestran direcciones MAC, y entre ellas la del 'destino', no es el equipo final, sino el router que se utiliza como puerta de enlace. Por lo que no es posible conocer la MAC de la universidad.

Conexiones TCP

- c) ¿Cuántas conexiones TCP se establecen con la página web de la Universidad? ¿Y cierres de conexión? ¿Por qué lo sabes? **(0.5 puntos)**

Si establecemos el filtro `tcp.flags.syn == 1`, filtraremos por aquellos paquetes TCP que tengan en flag SYN a 1. Contando éstos paquetes obtenemos 26 conexiones TCP con la universidad.

Para obtener los cierres de conexión, utilizamos un filtro similar `tcp.flags.fin == 1`. Volvemos a contar y obtenemos 13 fines de conexión.

Puerto petición web

- d) ¿A qué puerto se realiza la petición para obtener la página web? ¿A qué puerto/s se contesta? **(0.5 puntos)**

Buscamos paquetes HTTP, entre los primeros encontramos una petición del puerto 51916 al 80, y posteriormente, la respuesta del 80 al 51916.

PUSH

- e) ¿Hay algún segmento TCP que contenga el bit PUSH a 1? ¿Detectas en la captura alguna característica o patrón común en todos estos mensajes? ¿Por qué crees que puede ocurrir? **(0.5 puntos)**

Utilizamos un filtro `tcp.flags.psh == 1`, con el que obtenemos numerosos paquetes con el bit PUSH a 1. Analizándolos, podemos observar que van acompañados de comunicaciones con la aplicación.

Al recibir un paquete, sus datos quedan almacenados en un buffer, la señal del bit PUSH corresponde a la orden de vaciar el buffer y entregar su contenido a la aplicación.

Ejercicio 4 (2,5 puntos)

Utiliza Wireshark para realizar capturas de tráfico de diferentes protocolos. Para realizar esta captura es aconsejable tener cerradas todas las aplicaciones que puedan generar tráfico en segundo plano. Dichas capturas deberán ser filtradas mediante los comandos adecuados y exportadas mediante la instrucción *File/Export Specified Packets...* de tal forma que en ellas únicamente quede el tráfico intercambiado entre el ordenador original y el equipo de destino en un archivo de formato *.pcap*. El resultado obtenido deberá ser subido a la entrega habilitada en el campus virtual, con el nombre "Protocolo_*nombrequelprotocolo*.tcap". Además de la captura, será necesario especificar en el presente documento cómo se ha hecho para obtener la captura de cada uno de los protocolos.

Nota: Si por razones de privacidad no se desean subir las capturas *pcap* a la entrega del campus, las respuestas a todas las cuestiones deberán adjuntar capturas de pantalla con la información sensible tapada, pero donde se pueda observar claramente la captura obtenida.

ARP

a) Protocolo ARP. (0.5 puntos)

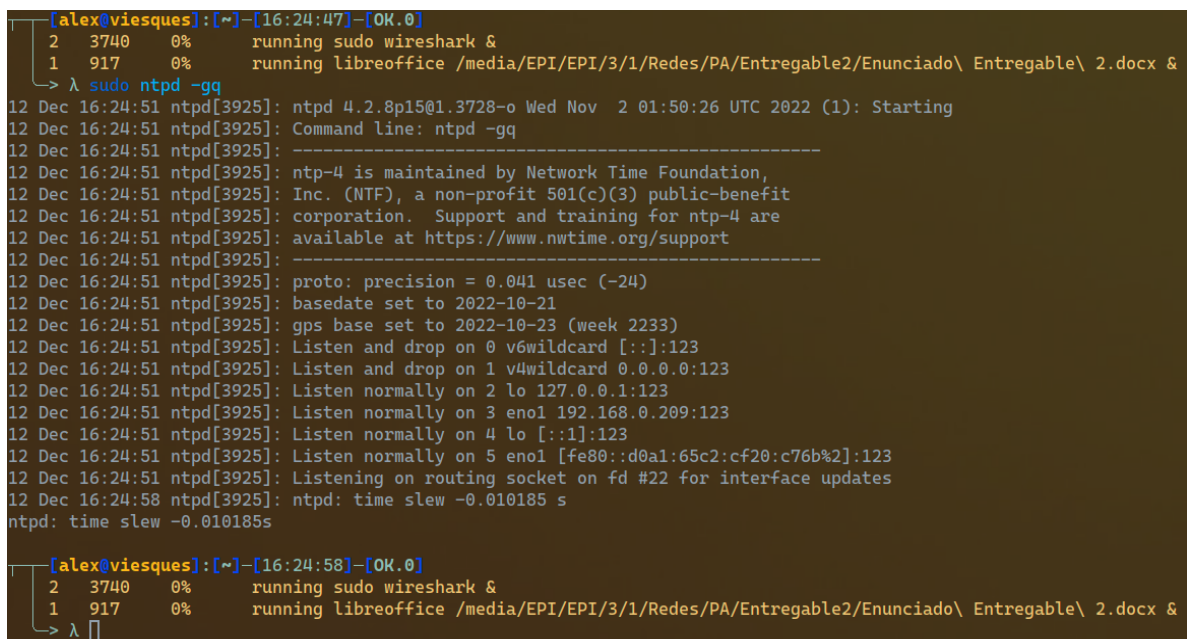
El protocolo ARP se produce al iniciar una comunicación a un equipo que no es conocido por el origen. Por ello, es muy simple obtener un ARP utilizando máquinas virtuales recién creadas. Ya que no se conocen entre ellas, la primera vez que hagamos ping a una, será necesario un ARP.

NTP

b) Protocolo NTP. (0.5 puntos)

El protocolo NTP se produce al iniciar el proceso que se encarga del NTP. En cualquier sistema Linux, solicitamos al demonio *ntpd* que corrija la fecha.

```
# ntpd -gq
```



```
[alex@viesques]:[~]-[16:24:47]-[OK.0]
2 3740 0% running sudo wireshark &
1 917 0% running libreoffice /media/EPI/EPI/3/1/Redes/PA/Entregable2/Enunciado\ Entregable\ 2.docx &
-> λ sudo ntpd -gq
12 Dec 16:24:51 ntpd[3925]: ntpd 4.2.8p15@1.3728-o Wed Nov 2 01:50:26 UTC 2022 (1): Starting
12 Dec 16:24:51 ntpd[3925]: Command line: ntpd -gq
12 Dec 16:24:51 ntpd[3925]: -----
12 Dec 16:24:51 ntpd[3925]: ntp-4 is maintained by Network Time Foundation,
12 Dec 16:24:51 ntpd[3925]: Inc. (NTF), a non-profit 501(c)(3) public-benefit
12 Dec 16:24:51 ntpd[3925]: corporation. Support and training for ntp-4 are
12 Dec 16:24:51 ntpd[3925]: available at https://www.nwtime.org/support
12 Dec 16:24:51 ntpd[3925]: -----
12 Dec 16:24:51 ntpd[3925]: proto: precision = 0.041 usec (-24)
12 Dec 16:24:51 ntpd[3925]: basedate set to 2022-10-21
12 Dec 16:24:51 ntpd[3925]: gps base set to 2022-10-23 (week 2233)
12 Dec 16:24:51 ntpd[3925]: Listen and drop on 0 v6wildcard [::]:123
12 Dec 16:24:51 ntpd[3925]: Listen and drop on 1 v4wildcard 0.0.0.0:123
12 Dec 16:24:51 ntpd[3925]: Listen normally on 2 lo 127.0.0.1:123
12 Dec 16:24:51 ntpd[3925]: Listen normally on 3 eno1 192.168.0.209:123
12 Dec 16:24:51 ntpd[3925]: Listen normally on 4 lo [::1]:123
12 Dec 16:24:51 ntpd[3925]: Listen normally on 5 eno1 [fe80::d0a1:65c2:cf20:c76b%2]:123
12 Dec 16:24:51 ntpd[3925]: Listening on routing socket on fd #22 for interface updates
12 Dec 16:24:58 ntpd[3925]: ntpd: time slew -0.010185 s
ntpd: time slew -0.010185s

[alex@viesques]:[~]-[16:24:58]-[OK.0]
2 3740 0% running sudo wireshark &
1 917 0% running libreoffice /media/EPI/EPI/3/1/Redes/PA/Entregable2/Enunciado\ Entregable\ 2.docx &
-> λ
```

Screenshot 2: *ntpd -gq*

DHCP

c) Protocolo DHCP. (0.5 puntos)

El protocolo DHCP se encarga de asignar direcciones IP a los equipos que se conecten a la red. En los sistemas Linux, dhcpd es el proceso que recibe la dirección IP del servidor DHCP. En situaciones normales, tratará de dar siempre la misma dirección, pero no es seguro. Utilizando dhcpd se puede solicitar la renovación de la IP utilizando:

```
# dhcpd -N <interfaz_red>
```

```
[alex@viesques]:[~]-[16:28:46]-[OK.0]
2 3740 0% running sudo wireshark &
1 917 0% running libreoffice /media/EPI/EPI/3/1/Redes/PA/Entregable2/Enunciado\ Entregable\ 2.docx &
> λ sudo dhcpd -N eno1
dhcpd-9.4.1 starting
DUID 00:04:bf:f4:4c:f8:99:5d:89:0a:b8:20:a8:5e:45:6b:eb:47
eno1: IAID 45:6b:eb:47
eno1: soliciting an IPv6 router
eno1: rebinding lease of 192.168.0.209
eno1: leased 192.168.0.209 for 604800 seconds
eno1: adding route to 192.168.0.0/24
eno1: adding default route via 192.168.0.1
forked to background, child pid 4552

[alex@viesques]:[~]-[16:28:53]-[OK.0]
2 3740 0% running sudo wireshark &
1 917 0% running libreoffice /media/EPI/EPI/3/1/Redes/PA/Entregable2/Enunciado\ Entregable\ 2.docx &
> λ ps uaxw | grep 4552
dhcpd 4552 0.0 0.0 3008 1360 ? S 16:28 0:00 dhcpd: eno1 [ip4] [ip6]
alex 4618 0.0 0.0 6956 2344 pts/0 S+ 16:29 0:00 grep --color=auto 4552
```

Screenshot 3: dhcpd -N eno1

DNS

c) Protocolo DNS. (0.5 puntos)

El protocolo DNS se encarga de resolver nombres de dominio. Esto es, convierte un nombre a una IP. Se puede obtener desde cualquier sistema entrando a cualquier página web utilizando su nombre, o alternativamente:

```
$ ping www.alexrl.es
```

```
[alex@viesques]:[~]-[16:33:40]-[OK.0]
2 3740 0% running sudo wireshark &
1 917 0% running libreoffice /media/EPI/EPI/3/1/Redes/PA/Entregable2/Enunciado\ Entregable\ 2.docx &
> λ ping www.alexrl.com
PING us-east-1.route-1.000webhost.awex.io (145.14.145.76) 56(84) bytes of data.
```

Screenshot 4: ping www.alexrl.com

SMTP/POP3/IMAP

d) Protocolo de correo electrónico (SMTP, POP3, IMAP...). (0.5 puntos)

Los paquetes de tipo SMTP, POP3 e IMAP están relacionados con el correo electrónico. Para recibir uno de ellos (por ejemplo el SMTP), se puede utilizar telnet:

```
[alex@viesques]:[~]-[17:14:06]-[OK.0]
> λ telnet smtp.gmail.com 587
Trying 173.194.76.109...
Connected to smtp.gmail.com.
```

Screenshot 5: telnet smtp.gmail.com 587