Enrutamiento y NAT

Área de Arquitectura y Tecnología de Computadores – Versión 1.0.915, 24/03/2022

Objetivos

El objetivo de esta sesión es doble. Por un lado pretende explicar los efectos del enrutamiento en la capa de enlace, analizando cómo un enrutador modifica las tramas que recibe de una red y que retransmite a otra. Por otro lado persigue explicar el funcionamiento del protocolo NAT (*Network Address Translation*), usado muy frecuentemente en IPv4. Comenzaremos justificando el porqué de su uso, cada vez más extendido para la creación de redes domésticas o de oficina. Trataremos de entender su funcionamiento analizando tramas con *Wireshark* y, finalmente, mostraremos algunos de los problemas que aparecen con su uso, así cómo las soluciones.

Conocimientos y materiales necesarios

Antes de comenzar esta práctica el alumno debe:

- Conocer la organización en capas de los protocolos de red.
- Conocer el formato de trama del protocolo de la capa de enlace Ethernet, la capa de red IP, la capa de transporte TCP y la capa de aplicación HTTP.
- Acudir al laboratorio de prácticas con el libro de apuntes de la asignatura.
- Durante la sesión se plantearán una serie de preguntas que puedes responder en el correspondiente cuestionario en el Campus Virtual. Puedes abrir el cuestionario en otra pestaña del navegador pinchando en el enlace mientras mantienes pulsada la tecla `Ctrl`.

1. Efectos del enrutamiento en la capa de enlace

Los enrutadores son equipos que permiten conectar varias redes entre sí. Cada paquete que llega a un enrutador, proveniente de una de las redes a las que está conectado, es analizado para conocer su dirección IP destino reenviado (o retransmitido) hacia otra de sus redes en dirección al destinatario. Lo normal es que después de pasar por varios enrutadores el paquete llegue a su destino, es decir, al equipo cuya dirección IP coincide con la dirección IP destino del paquete.

Los enrutadores son dispositivos que trabajan en la capa de red, implementan complejos algoritmos de enrutado y almacenan grandes tablas de enrutamiento. En general, ignoran lo que ocurre en las capas física y de enlace. No obstante, cada una de las interfaces de red de un enrutador está conectada a una red diferente, por lo que las direcciones MAC de las tramas deben modificarse cuando pasan a través de un enrutador. Recuerda que las direcciones MAC se usan para direccionar dispositivos dentro de la misma red local.

La figura 1 muestra un servidor web y un cliente web conectados a través de un enrutador. Tanto el equipo que ejecuta el cliente como el que ejecuta el servidor web se han configurado con la máscara de red 255.255.255.0. El equipo cliente usa como puerta de enlace la dirección 192.168.2.1, mientras que el servidor web utiliza como puerta de enlace la dirección 156.35.86.150. Se ha instalado *Wireshark* tanto en el equipo servidor como en el cliente, y se han realizado dos capturas simultaneas empleando el filtro `http tcp port (80)`, es decir, solo se capturan las tramas que incorporan TCP/IP y el puerto 80. A continuación se ha accedido a través de un navegador web en el cliente a una página web del servidor. Las capturas obtenidas a ambos lados del enrutador se denominan `cliente-privada.pcap` y `servidor-publica.pcap` (como se observa en la figura), y ambas forman parte de los archivos proporcionados para esta sesión práctica.

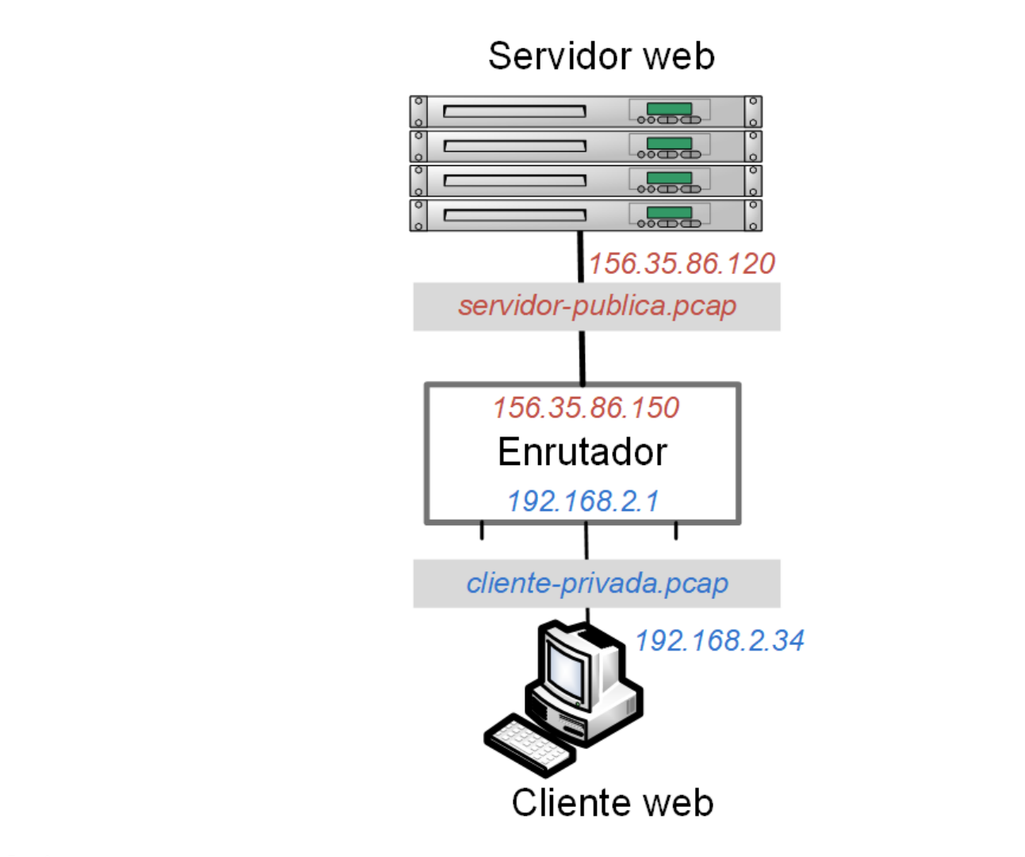

Figura 1. Configuración del sistema

- Ejecuta *Wireshark* y abre el archivo `cliente-privada.pcap`. En el menú, selecciona la opción **Edit › Preferences › Name Resolution** y desactiva la opción **Resolve MAC address**.
- Ejecuta una segunda instancia de *Wireshark* y abre desde la misma el archivo de captura `servidor-publica.pcap`. En el menú, selecciona la opción **Edit › Preferences › Name Resolution** y desactiva la opción **Resolve MAC address**. El objetivo de tener dos instancias de *Wireshark* es facilitar la comparación de las capturas realizadas por el cliente y el servidor.
- En la primera instancia de *Wireshark*, la correspondiente al cliente web, selecciona la primera trama en el panel superior y, en el panel intermedio, selecciona la capa Ethernet. Expande la información pulsando la tecla `>`.
- ¿Cuál es la dirección MAC de origen? ¿Con qué interfaz de red se corresponde? Para responder a ambas preguntas, escribe la dirección MAC en el hueco apropiado de la figura 2.
- ¿Cuál es la dirección MAC de destino? ¿Con qué interfaz de red se corresponde? Para responder a ambas preguntas, escribe la dirección MAC en el hueco apropiado de la figura 2.

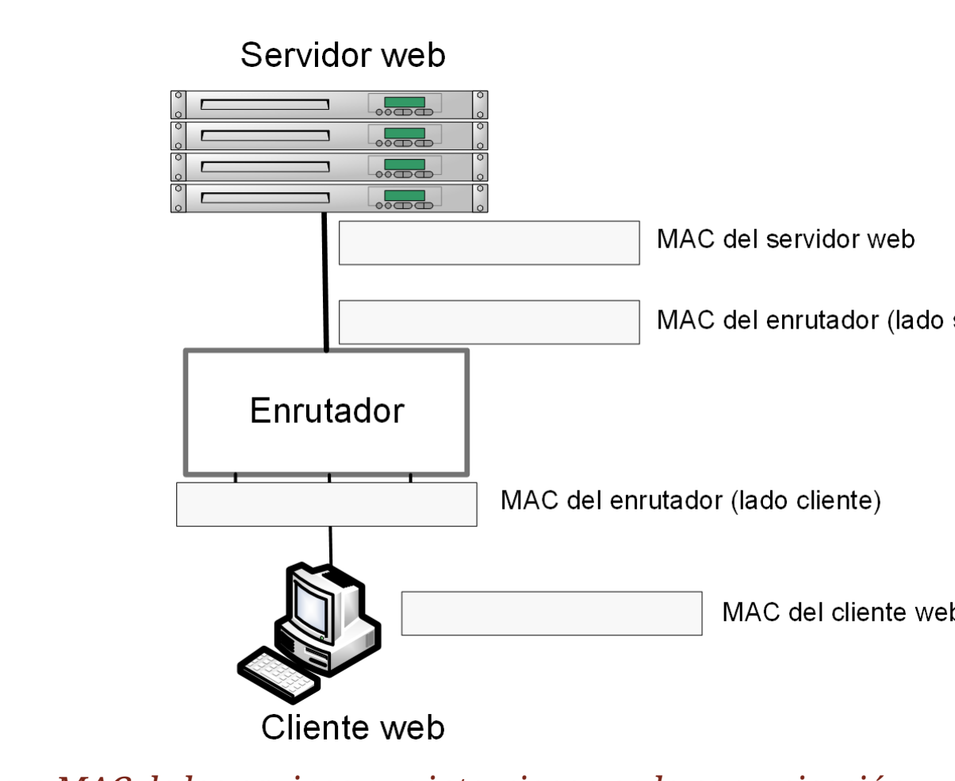

Figura 2. Direcciones MAC de los equipos que intervienen en la comunicación

- Puesto que la trama anterior debe llegar al servidor web, el cual se encuentra en otra red, la dirección MAC de destino debe coincidir con la de la puerta de enlace. ¿Qué dirección IP está asociada a la dirección MAC anterior? Responde en el cuestionario: pregunta 1. Por lo tanto, ¿qué interfaz de red hace de puerta de enlace de la red a la que está conectada el cliente web? Responde en el cuestionario: pregunta 2.
- Observa, en las siete tramas restantes, cómo todas emplean las mismas direcciones MAC.
- Céntrate ahora en la segunda instancia de *Wireshark*. Selecciona, en el primer panel, la primera trama y, en el panel intermedio, la capa Ethernet. Expande la información pulsando la tecla `+`.
- ¿Cuál es la dirección MAC de origen? ¿Con qué interfaz de red se corresponde? Para responder a ambas preguntas, escribe la la dirección MAC en el hueco apropiado de la figura 2.
- ¿Cuál es la dirección MAC de destino? ¿Con qué interfaz de red se corresponde? Para responder a ambas preguntas, escribe la dirección MAC en el hueco apropiado de la figura 2.
- Como habrás observado, las direcciones MAC fuente y destino de las tramas que atraviesan el enrutador desde el cliente al servidor web, y viceversa, se modifican a su paso. Cada vez que una trama llega a un enrutador desde una red y deba ser retransmitida a un equipo en otra red, el enrutador debe llevar a cabo esos reemplazos para que exista conectividad a nivel de capa de enlace: las tramas deben llevar siempre las dirección MAC de los equipos que intercambian las tramas (dentro de la misma red) y estos cambian al pasar de la red privada a la pública y viceversa. Si no se hiciesen estos cambios los equipos que deberían recibir las tramas las ignorarían.

Si te fijas en las direcciones IP fuente y destino en la segunda instancia de *Wireshark*, capturada en el servidor, verás que la dirección IP asociada al cliente web no se corresponde con la asignada según la primera instancia de *Wireshark*. Esta es una de las funcionalidades del protocolo NAT, que estudiaremos a continuación.

No cierres estas dos instancias de *Wireshark* porque las vas a utilizar más adelante en esta práctica.

2. Introducción a NAT

Uno de los principales problemas del protocolo IP en su versión 4, denominado IPv4, es el limitado número de direcciones IP que proporciona. Las direcciones IPv4 se codifican con 32 bits, por lo que en principio se dispone de 2^{32} direcciones diferentes, aproximadamente 4300 millones. Teniendo en cuenta la población mundial actual, unos 7000 millones de habitantes, y sabiendo que cada ordenador personal, tableta y buena parte de los móviles actuales requieren una dirección IP, resulta claro el problema de agotamiento de las direcciones IP. Además, parte de las direcciones IP están reservadas para usos especiales y las que están disponibles se asignan por grupos a empresas e instituciones.

La solución definitiva a los problemas de IPv4 pasa por la implementación de una nueva revisión que incluya un rango de direcciones mayor. La última versión del protocolo IP, IPv6, utiliza direcciones de 128 bits, por lo que se pueden direccionar 2^{128} elementos diferentes en la red. Aunque la versión 6 del protocolo IP está diseñada para sustituir a la versión 4, aún son pocos dispositivos los que la utilizan. En cualquier caso, con IPv4 se utiliza el protocolo NAT (*Network Address Translation*), que permite solucionar el problema hasta que se utilice IPv6 en toda la red.

La idea fundamental que persigue NAT es conseguir que varios equipos puedan compartir una o más direcciones IP de forma totalmente transparente. Es decir, como si tuviesen una dirección IP diferente cada uno, aunque desde el punto de vista de la red global solo están utilizando una única dirección IP. Aunque NAT se acerca a este ideal en gran medida, tal como veremos este objetivo no se logra al 100%.

Asociado a NAT aparecen dos tipos de direcciones IP: **direcciones privadas** y **direcciones públicas**. Las direcciones privadas son las direcciones IP asociadas a los equipos conectados a la red a través de NAT. El conjunto de todos estos equipos y sus direcciones privadas constituye lo que se denomina una **red privada**. La figura 3 muestra un ejemplo de tres redes privadas conectadas a Internet a través de tres enrutadores que implementan NAT. Como se puede observar, podemos tener equipos con la misma dirección IP (privada) en diferentes redes privadas, por lo que el número de equipos conectados a Internet podría ser prácticamente ilimitado. La dirección IP se denomina privada pues solo es visible a los dispositivos conectados dentro de la misma red privada. Fuera de la misma, la única dirección IP que se observa es la dirección IP pública asociada al enrutador con NAT.

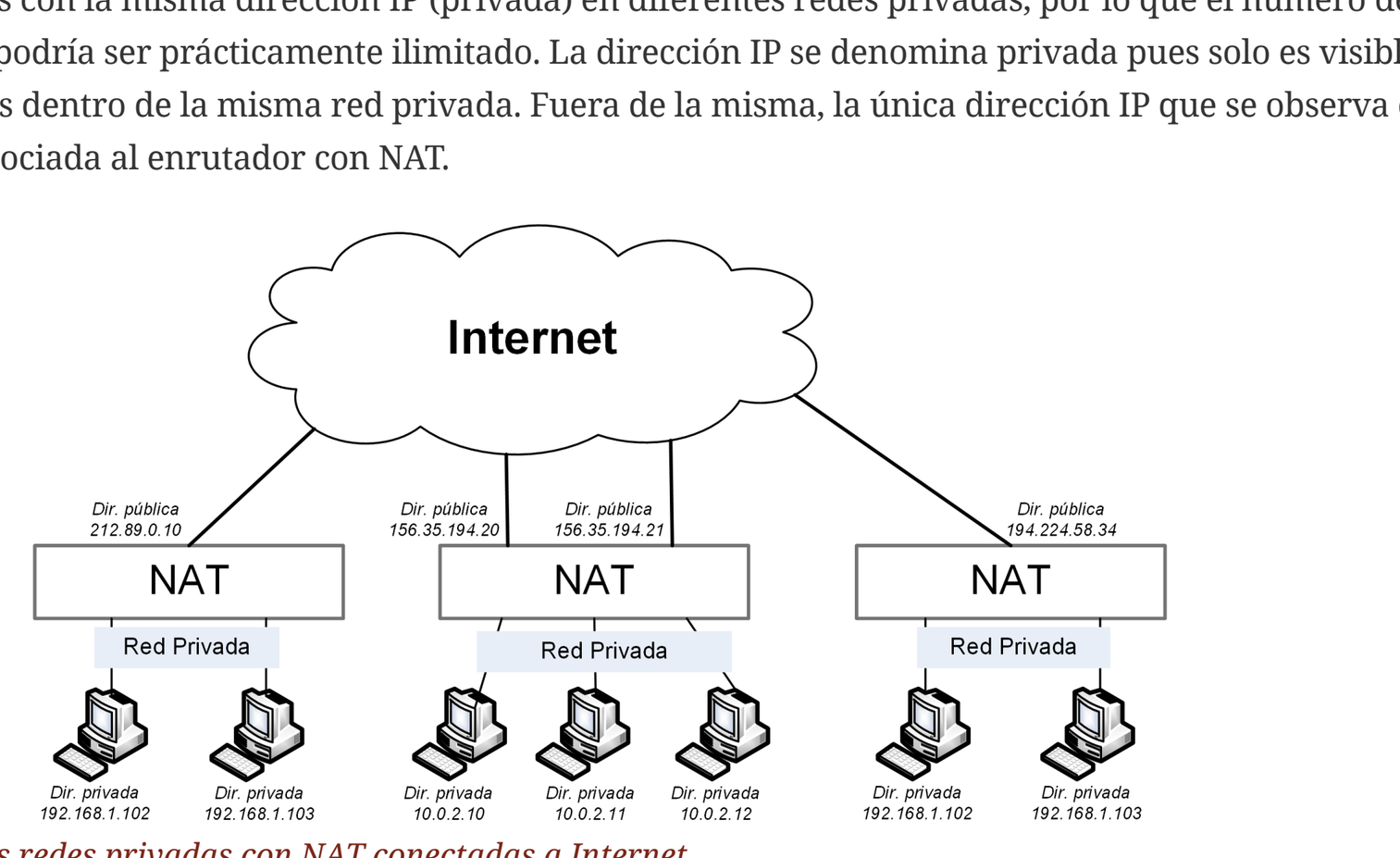

Figura 3. Ejemplo de tres redes privadas con NAT conectadas a Internet

Los enrutadores no solo incorporan la funcionalidad NAT, sino también un gran número de características entre las que se incluyen:

- Enrutamiento entre todas sus interfaces de red. Habitualmente incorporan dos interfaces Ethernet, una para conectarse a la red privada y otra para conectarse a la red pública, así como una interfaz Wi-Fi, cada una con sus direcciones MAC e IP.
- Servidor DHCP para los equipos conectados a la red privada.
- Funciones de conmutador, o *switch*, para todas las interfaces de su red privada.
- Redirección de puertos, *port forwarding* o *tunneling*. Esta funcionalidad permite redirigir paquetes a un puerto concreto de una dirección IP privada.
- Configuración a través de web [1].
- Gestión de la calidad de servicio.

La figura 4 muestra un ejemplo de enrutador con funcionalidad NAT.

Figura 4. Ejemplo de enrutador doméstico con NAT

La implementación más habitual de NAT se basa en la traducción de puertos, y recibe el nombre de NAPT (*Network Address and Port Translation*). Para comprender su funcionamiento consideremos el caso más frecuente, en el cual todos los equipos de una red privada comparten una única dirección IP pública: la dirección IP pública del enrutador con NAT. Por ejemplo, supongamos que un navegador web se ejecuta sobre el equipo de dirección 192.168.1.103 (cliente web) y trata de conectarse desde el puerto 2600, del protocolo TCP, a un servidor web de dirección 156.35.33.99 usando como puerto destino el puerto por defecto de un servidor HTTP: TCP 80. Supongamos además que la dirección IP pública del enrutador NAT es 194.224.58.34. Básicamente, el enrutador lleva a cabo las siguientes operaciones, ilustradas en la parte izquierda de la figura 5:

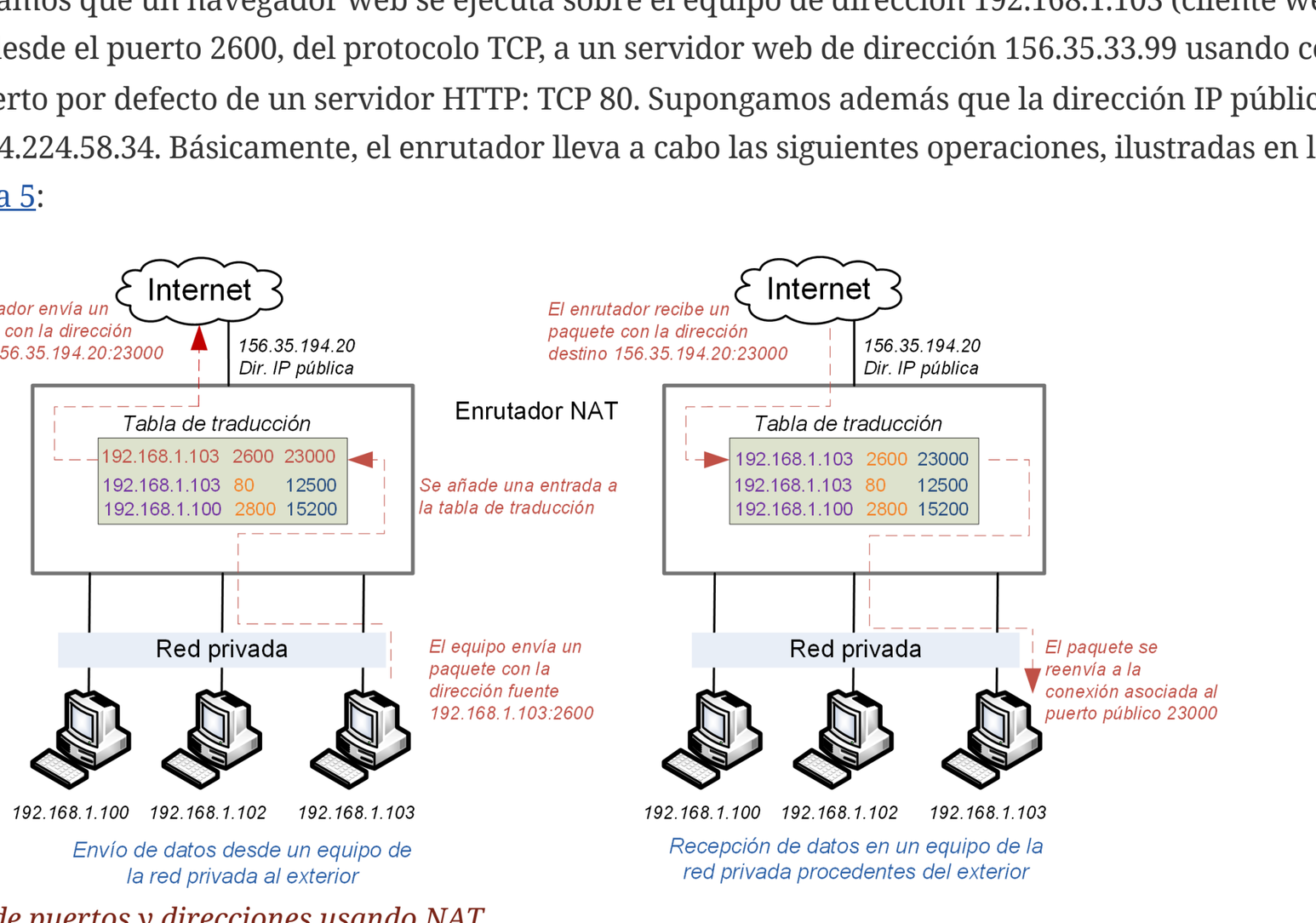

Figura 5. Traducción de puertos y direcciones usando NAT

- Sustituye la dirección IP privada 192.168.1.103 del paquete de datos por la dirección IP pública 156.35.194.20.
- Sustituye el puerto fuente 2600 del paquete de datos por un nuevo puerto fuente, por ejemplo el 23000.
- En una tabla interna, denominada tabla de traducción, crea una fila con la siguiente información:

Dirección IP privada	Puerto privado	Puerto público
192.168.1.103	2600	23000

  El puerto público 23000 es un puerto libre que no se ha usado como puerto público en otras entradas de la tabla de traducción [2].
- El enrutador NAT envía el paquete traducido a través de su boca de red pública y el servidor web acabará recibiendo un paquete de datos de la dirección 156.35.194.20:23000. Observa cómo se representa de forma compacta la dirección completa, formada por la dirección IP y el puerto.

Al cabo de un cierto tiempo, el servidor web responderá con un paquete de datos para la dirección 156.35.194.20:23000. Una vez el enrutador NAT recibe este paquete de datos, lleva a cabo las siguientes operaciones, mostradas en la parte derecha de la figura 5:

1. Busca en la tabla de traducción una entrada con el número de puerto público 23000. Observa entonces que tiene asociada la dirección IP privada 192.168.1.103 y el puerto privado 2600.
2. Sustituye la dirección IP de destino del paquete de datos, 156.35.194.20, por la dirección IP privada 192.168.1.103.
3. Sustituye el puerto de destino del paquete de datos, 23000, por el puerto privado 2600.
4. Envía el paquete IP traducido, es decir, el que tiene dirección destino 192.168.1.103:2600 a la boca de red en la que se encuentra la conexión del navegador web del equipo con dirección IP privada 192.168.1.103.

3. Análisis básico del proceso de traducción

Una vez conocemos el principio de funcionamiento de NAT vamos a llevar a cabo un análisis preliminar del proceso de traducción empleando *Wireshark*. Sobre el sistema mostrado en la figura 6, en la cual se puede observar un servidor web y un cliente web conectados a través de un enrutador NAT, se han realizado capturas de tramas con *Wireshark*. El sistema es el mismo utilizado en el primer ejemplo de esta sesión. El servidor web se conecta a la parte pública de red, mientras que el cliente web se conecta a la parte privada de red. El cliente web accede con su navegador al servidor web, y el resultado se muestra en la parte inferior derecha de la figura.

Figura 6. Configuración del sistema para el análisis de NAT

Vamos a utilizar las dos instancias de *Wireshark* que mantienes abiertas. La primera instancia muestra el contenido del fichero `cliente-privada.pcap` y la segunda el de `servidor-publica.pcap`. Si las has cerrado anteriormente, ábrelas tal cual se describe en la sección Efectos del enrutamiento en la capa de enlace.

- La trama número 4 de ambas capturas coincide con el envío de una petición de una página web desde el cliente hacia el servidor web. ¿Cuál es la dirección IP destino en ambas tramas? Responde en el cuestionario: pregunta 3. ¿Con la de qué equipo coincide? Responde en el cuestionario: pregunta 4. El enrutador cambiará esta dirección por su dirección IP pública antes de reenviar el datagrama.

Una vez conocemos el funcionamiento básico de los enrutadores NAT, vamos a ver su actuación en las diferentes capas, desde la capa de red a la capa de aplicación.

4. Traducción NAT en la capa de red

En este apartado veremos cómo NAT lleva a cabo traducciones dentro de la capa de red, especialmente en todo lo relacionado con direcciones IP.

- En la primera instancia de *Wireshark*, la correspondiente al cliente web, selecciona la primera trama y expande en el segundo panel la información de la capa IP.
- ¿Cuál es la dirección IP de origen? Responde en el cuestionario: pregunta 5. ¿Con qué interfaz de red se corresponde? Responde en el cuestionario: pregunta 6.
- ¿Cuál es la dirección IP de destino? Responde en el cuestionario: pregunta 7. ¿Con qué interfaz de red se corresponde? Responde en el cuestionario: pregunta 8.
- Como podrás observar, la dirección IP destino de la trama está asociada al servidor web, mientras que la dirección MAC destino de la trama se corresponde con la de otro equipo (la interfaz de red privada del enrutador). Esto es así porque la dirección MAC se emplea para enviar información entre dos equipos dentro del mismo segmento de red, mientras que la dirección IP sirve para enrutarla a través de varios segmentos hasta el equipo destino. En este caso, tal como comentamos en el apartado anterior, la dirección MAC se emplea para llevar la trama hasta la puerta de enlace (la interfaz de red privada del enrutador).
- ¿Cuál es el tiempo de vida (TTL) del paquete? Responde en el cuestionario: pregunta 9.
- En la segunda instancia de *Wireshark*, la correspondiente al servidor web, selecciona el primer paquete, y expande en el segundo panel la información de la capa IP.
- ¿Cuál es la dirección IP de origen? Responde en el cuestionario: pregunta 10. ¿Con qué interfaz de red se corresponde? Responde en el cuestionario: pregunta 11.
- ¿Cuál es la dirección IP de destino? Responde en el cuestionario: pregunta 12. ¿Con qué interfaz de red se corresponde? Responde en el cuestionario: pregunta 13.
- ¿Cuál es el tiempo de vida (TTL) del paquete? Responde en el cuestionario: pregunta 14. Fíjate que es una unidad menos que el tiempo de vida del paquete original, ya que el enrutador lo decrementó antes de reenviar el datagrama.
- Cada vez que un paquete llega a un enrutador sin funcionalidad NAT desde una red y debe transmitirlo a un equipo en otra red, las direcciones IP fuente y destino no cambian. ¿Se cumple esto con el enrutador NAT empleado? Responde en el cuestionario: pregunta 15. ¿Qué dirección IP se reemplaza? Responde en el cuestionario: pregunta 16. ¿Por qué dirección IP es reemplazada? Responde en el cuestionario: pregunta 17.
- Desde el punto de vista del servidor web, ¿qué equipo percibe como cliente web? Responde en el cuestionario: pregunta 18.

5. Ejercicios adicionales

✓ Observando la captura realizada por el cliente web, `cliente-privada.pcap`, ¿podrías decir si el cliente web se cerró antes de terminar la captura? Responde en el cuestionario: pregunta 19.

✓ Dentro de la capa de red se encuentra un campo *checksum*. ¿Cuáles son los valores para el primer paquete de las capturas `cliente-privada.pcap` y `servidor-publica.pcap`? Responde en el cuestionario: pregunta 20. Los valores han cambiado porque dos campos en el datagrama han cambiado: la dirección que se ha traducido y el TTL. Si no se actualizase el checksum, el datagrama sería considerado inválido y sería rechazado.

1. Por ejemplo, si la puerta de enlace de los equipos conectados a la red privada tiene la IP 192.168.2.1, se puede acceder a la configuración del enrutador accediendo al recurso http://192.168.2.1 desde un navegador web ejecutándose en cualquier equipo de su red privada.
2. Muchos enrutadores NAT usan como puerto público el número de puerto privado, salvo que ya haya sido usado previamente por otro equipo de la red privada, reduciendo de esta forma el tamaño de la tabla de traducción.