

Práctica 5: NAT: funcionamiento y análisis de trazas

Lectura previa: Kurose 7ª edición, apartado 4.3.4 (páginas 286 – 288)

Video: <https://www.youtube.com/watch?v=hBloGXo2DIY>

Trabajo previo antes de la sesión de laboratorio:

- Lectura y comprensión de los apartados 1. Introducción y 2. Traducción de direcciones de red.
- Resolución del Ejercicio 1

1. Introducción

En esta práctica vamos a estudiar el funcionamiento del mecanismo NAT, o traducción de direcciones IP.

El mecanismo NAT nace como respuesta a la proliferación de pequeñas redes domésticas y de oficina con conexión a Internet. Cuando se contratan los servicios básicos de un ISP, éste nos proporciona una conexión a Internet con un ancho de banda determinado (de acuerdo al contrato elegido) y una única dirección IP con la que podemos identificarnos en Internet.

Esta configuración es suficiente si queremos conectar un único ordenador a Internet. Sin embargo, en el caso habitual de disponer de una pequeña red de área local y desear que los diferentes ordenadores de la misma puedan acceder a Internet simultáneamente, los servicios que nos proporciona el ISP no son suficientes. Más concretamente, el hecho de disponer de una única dirección IP (o hablando en términos más generales, de disponer de menos direcciones IP que ordenadores) nos crea el problema de que no todos los ordenadores de nuestra red van a poder conectarse a Internet de forma simultánea ya que no tienen una dirección IP con la que identificarse.

Una solución a este problema sería contratar un pequeño rango de direcciones IP para casa o la oficina. Pero esta opción, además de ser notablemente más costosa que una única dirección IP, conlleva además la necesidad de gestionar un router, lo cual queda fuera del alcance de los conocimientos de la mayoría de usuarios de Internet.

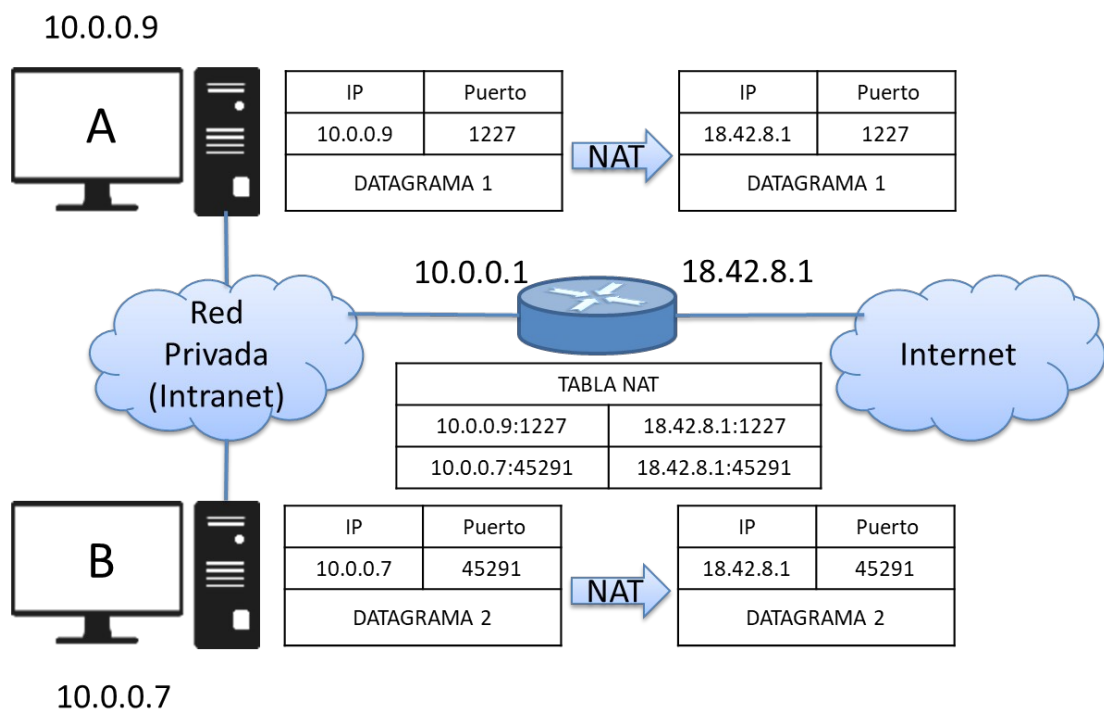
Una mejor opción es seguir contratando una única dirección IP e idear algún mecanismo para compartir esa dirección que nos ha proporcionado el ISP entre los ordenadores de la red de casa o de la oficina. Este mecanismo se conoce como traducción de direcciones, o NAT (*Network Address Translation*).

2. Traducción de direcciones de red

El mecanismo de traducción de direcciones de red (NAT) se complementa generalmente con el uso de direcciones privadas, de forma que es habitual encontrar dicho tipo de direcciones en la red local de casa o de la oficina (también conocida como intranet) que usan este mecanismo para acceder a Internet. No obstante, el funcionamiento del mecanismo es independiente del tipo de direcciones que se use en la intranet.

A modo de resumen (estudiar la sección 4.3.4 del Kurose para una información más detallada), el funcionamiento del mecanismo NAT es como sigue. Tal y como se muestra en la figura siguiente, cuando un ordenador de la red local accede a un servidor en Internet, envía el correspondiente datagrama al dispositivo NAT (también conocido como *router* NAT, a pesar de que sus funciones quedan lejos de las de un *router*). El *router* NAT actúa como puerta de enlace de la red local. Este dispositivo cambia la dirección origen del datagrama, que será en general una dirección privada, por la dirección pública que ha facilitado el ISP. Asimismo, en caso necesario (si el puerto ya está en uso en otro ordenador de la red interna), cambia el puerto origen del segmento TCP o del datagrama UDP por uno nuevo, con el fin de poder reenviar posteriormente la respuesta del servidor al host que originó la petición.



Durante el proceso de traducción el dispositivo NAT guarda en una tabla (tabla de traducciones) la equivalencia entre el puerto origen inicial y el nuevo puerto origen para cada uno de los datagramas que lo atraviesa. De esta forma, cuando llega una respuesta desde Internet, utiliza el puerto destino de la respuesta (puerto origen cambiado en la petición correspondiente anterior) para buscar en dicha tabla la entrada correspondiente y saber a qué host de la red local debe reenviar la respuesta del servidor. En el proceso de reenvío hacia el interior de la red local modifica la dirección destino y el puerto destino para que coincidan con los iniciales. En la figura siguiente se puede ver un ejemplo de la tabla de traducciones.



Ejercicio 1. Se pretende configurar manualmente la interfaz de la red pública de un dispositivo NAT con los siguientes valores:

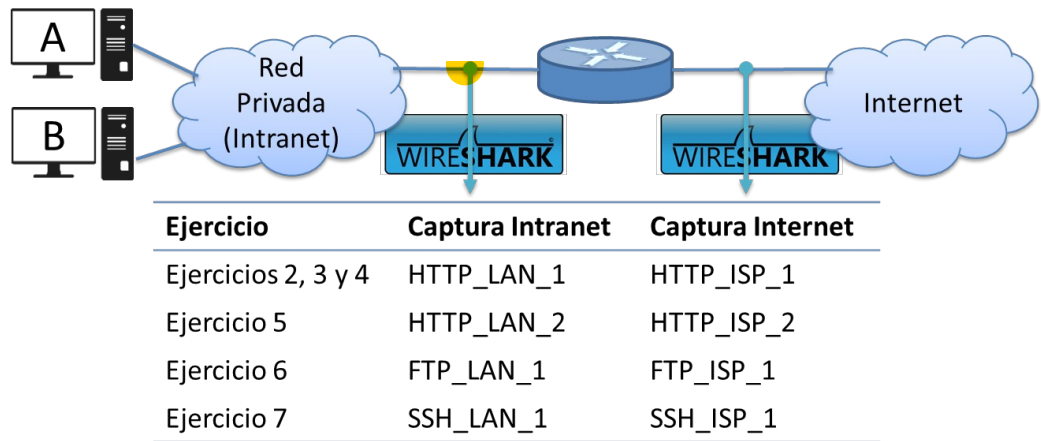
Dirección IP pública:	158.42.180.1
Máscara de subred:	255.255.255.0
Puerta de enlace:	158.42.181.250
Servidor de nombres 1:	158.42.249.8
Servidor de nombres 2:	158.42.1.8

Una vez introducidos esos valores, el dispositivo NAT nos dice que la dirección IP de la puerta de enlace es incorrecta. Sin embargo, tras comprobar los valores, tanto la dirección IP de la puerta de enlace como la dirección IP pública asignada al NAT son correctas.

1. ¿Por qué nos dice el NAT que la dirección IP de la puerta de enlace es incorrecta? 
2. ¿Qué parámetro habría que cambiar para que la configuración fuera correcta? Propón un valor para dicho parámetro que haga correcta la configuración. 
3. ¿Están los servidores DNS en la misma red que la interfaz configurada? En caso de no estarlo, ¿sería posible un correcto funcionamiento? Justifica la respuesta.

3. Análisis de tráfico

En esta sección vamos a analizar los paquetes que atraviesan un dispositivo NAT. En lugar de realizar nosotros las capturas de paquetes con el programa *Wireshark*®, vamos a usar unas capturas previamente realizadas y que están contenidas en los ficheros HTTP_LAN_1, HTTP_LAN_2, FTP_LAN_1, SSH_LAN_1 y también sus respectivas versiones en la parte del ISP. Estos ficheros se encuentran en PoliformaT. El motivo para utilizar unas capturas ya hechas es que, aunque podríamos fácilmente capturar el tráfico que genera nuestro ordenador en la red local, es complejo capturar el tráfico que sale del router NAT, dado que de normal no se tiene acceso a esa red. La siguiente figura muestra el escenario en el que vamos a trabajar.



Ejercicio 2. El fichero HTTP_LAN_1 contiene una captura de tráfico generado dentro de la LAN (intranet). Abre el fichero HTTP LAN 1 con *Wireshark* y responde a las siguientes cuestiones:

1. ¿Cuántas conexiones TCP se realizan? **2 conexiones TCP**
2. Localiza el datagrama que contiene la petición web "GET / HTTP/1.1". ¿Cuáles son las direcciones IP y números de puerto TCP utilizados? ¿Corresponden origen y destino a cliente y servidor web, respectivamente?
3. Localiza el datagrama que contiene la respuesta "HTTP 200 OK" enviada por el servidor web. ¿Las direcciones IP y números de puerto corresponden a los de cliente y servidor encontrados en la petición web anterior?
4. ¿Qué puertos se usan en la segunda conexión TCP?

Como puerto del servidor web: 80 y cliente: 39137

Ejercicio 3. Vamos a centrarnos ahora en los mensajes HTTP que salen y entran del router NAT hacia o desde el servidor web (red ISP). Para ello, abre el fichero HTTP ISP 1, donde se muestra el tráfico que se ha generado a la parte externa del router NAT (internet) a partir del tráfico generado en la intranet (captura anterior). *Nota: los tiempos de ambas capturas no están sincronizados.*

Localiza el mensaje de salida "GET / HTTP/1.1". Éste corresponde al reenvío por parte del router NAT del datagrama correspondiente generado en la intranet (ejercicio 2).

1. ¿En qué momento se transmite este mensaje? ¿Cuáles son las direcciones IP y números de puerto TCP utilizados? ¿Corresponden origen y destino a cliente y servidor web, respectivamente?
2. ¿Cuál es la dirección IP pública del router NAT?
3. Respecto del datagrama correspondiente de la intranet ¿ha cambiado algún campo del mensaje HTTP? ¿y de la cabecera del datagrama IP? Para aquellos campos que se han modificado ¿cuál es el motivo?

Localiza el mensaje de entrada "HTTP 200 OK" enviado por el servidor web.

4. ¿En qué momento se recibe este mensaje? ¿Cuáles son las direcciones IP origen y destino del datagrama que lo contiene? ¿Se corresponden con las observadas en el ejercicio 2?

Ejercicio 4. Basándote en la información observada en los dos ejercicios anteriores, rellena la tabla de traducciones del router NAT, donde se recogen las correspondencias entre direcciones IP y números de puerto a ambos lados del router NAT en las dos conexiones TCP.

Conexión	Entrada desde LAN		Salida a red ISP	
	IP origen	Puerto origen	IP origen	Puerto origen
1	192.168.1.181	52467	158.42.180.22	52467
2	192.168.1.181	39137	158.42.180.22	39137

Ejercicio 5. En el ejercicio anterior se ha podido ver que el router NAT ha mantenido los mismos números de puerto origen en los segmentos de salida. Esta política es tan válida como cualquier otra, siempre que se lleve cuidado de que si el puerto a usar ya está en la tabla de traducciones, entonces habrá que usar un número de puerto nuevo. Precisamente eso es lo que vamos a comprobar en este ejercicio. Vamos a provocar que el router NAT tenga que modificar el número de puerto origen porque el que necesita ya está en uso. Para ello, en dos ordenadores de la red privada vamos a ejecutar el siguiente programa:

```
import java.net.*;
import java.io.*;

class ClienteTCP {
    public static void main(String args[]) throws Exception {
        String mi_IP = "192.168.1.2";
        InetAddress DirIP = InetAddress.getByName(mi_IP);
        Socket s = new Socket("www.redes.upv.es", 80, DirIP, 40000);
        PrintWriter esc= new PrintWriter(s.getOutputStream(), true);
        esc.println("GET / HTTP/1.1");
        esc.println("Host: www.redes.upv.es");
        esc.println();
        while(true);
    }
}
```

La variable “mi_IP” contendrá la dirección IP del ordenador en cuestión donde se esté ejecutando el programa. Básicamente, este programa abre una conexión TCP con un servidor web y la mantiene abierta. De esta forma, cuando ejecutemos el mismo programa en el segundo ordenador, el *router* NAT verá que el puerto que necesita está ocupado y no tendrá más remedio que usar uno nuevo que esté libre.

Abre el fichero HTTP LAN 2, que corresponde al tráfico generado por uno de los ordenadores de la red privada (LAN) donde se ha ejecutado el programa anterior.

1. ¿Cuáles son las direcciones IP de cliente y servidor y los números de puerto utilizados por cada uno de ellos?



Abre el fichero HTTP ISP 2. Este fichero contiene el tráfico generado en la red pública (ISP) por los dos ordenadores que ejecutaron el programa anterior en la red privada.

2. ¿Qué número de puerto origen asigna el *router* NAT a los segmentos de salida a la red pública en cada una de las dos conexiones?
3. ¿Cómo sabemos cuál de las dos conexiones TCP corresponde a la contenida en el fichero HTTP_LAN_2? Sugerencia: revisa identificador del paquete IP.




Basándote en la información proporcionada, rellena la tabla de traducciones NAT:

Conexión	Entrada desde LAN		Salida a red ISP	
	IP origen	Puerto origen	IP origen	Puerto origen
1	192.168.1.2	40000	158.42.180.22	40000
2	192.168.1.2	40000	158.42.180.22	40016



Ejercicio 6. Hasta ahora hemos visto que el *router* NAT modifica los campos de la cabecera IP y de la cabecera TCP (o UDP). Pero en ocasiones también se ve obligado a modificar el contenido del mensaje que viaja en el segmento TCP. Estudia los ficheros FTP LAN 1 y FTP ISP 1.

1. ¿Cuáles son las direcciones IP de cliente y servidor *ftp*? 
2. Fíjate en uno cualquiera de los dos ficheros. Observarás que se establecen dos conexiones TCP ¿Para qué se usa cada una? Si no lo sabes revisa el funcionamiento básico del protocolo *ftp* ¿Cuáles son los números de puerto utilizados por cliente y servidor en cada una de las conexiones? Identifica los segmentos de fin de conexión de cada una de ellas.

Nota: en esta última pregunta, así como en el siguiente apartado, puedes ayudarte del filtro de pantalla para visualizar sólo una de las conexiones, por ejemplo, filtrando por número de puerto. Para ello escribe `tcp.port==Número_puerto`. Recuerda limpiar los filtros de visualización cuando termines de usarlos.

3. Fíjate en el datagrama que se genera en la red privada en el instante 4.307125 y compáralo con su correspondiente en la red externa. ¿Que cambia entre ambos? ¿Altera esto los números de secuencia de los subsiguientes segmentos TCP?

4. Servidores dentro de la intranet

Como hemos visto, NAT funciona de forma automática cuando un ordenador de la intranet se conecta a un servidor fuera de la intranet. Esto es así porque el *router* NAT modifica de forma automática los números de puerto de los segmentos que salen hacia el exterior, así como las direcciones IP de los datagramas que los contienen, guardando dichas correspondencias en su tabla de traducciones.

Sin embargo, si nos restringimos al procedimiento anterior, cuando se trata de acceder desde el exterior a un servidor en la intranet, no existirá ninguna correspondencia en la tabla y, por tanto, el *router* NAT no sabrá qué transformaciones debe realizar. Así pues, habrá que “enseñar” al *router* NAT lo que debe hacer con las peticiones entrantes hacia servidores internos. En particular, son necesarios dos pasos:

1. Hay que configurar el dispositivo NAT para que acepte peticiones destinadas al puerto del servidor y, además, cuando llegue una de estas peticiones, el dispositivo NAT debe saber a qué ordenador en la intranet debe reenviar la petición. Esto es lo que se conoce como *port forwarding*. Todo esto hay que configurarlo antes de poder dar servicio al exterior.
2. Dado que, en muchos casos, las direcciones IP de la intranet se asignan dinámicamente gracias a un servidor DHCP incorporado en el *router* NAT, debemos asegurarnos que el ordenador que haga de servidor siempre obtenga la misma dirección IP. Si no es así, cuando llegue una petición a un puerto del servidor, el *router* la reenviará a la dirección IP de la intranet que tenga configurada, pero el servidor puede no estar en esa dirección IP.

Ejercicio 7. En esta práctica no vamos a configurar un *router* NAT para que realice *port forwarding*, pero vamos a analizar los paquetes que llegan a un dispositivo NAT desde el exterior y que van destinados a un servidor *ssh* que está ejecutándose en un ordenador de la intranet. Para ello vamos a utilizar los ficheros de captura SSH LAN 1 y SSH ISP 1.

1. ¿Cuáles son las direcciones IP de cliente y servidor **ssh** y los números de puerto utilizados por cada uno de ellos?
2. ¿Qué diferencias observas en los datagramas y segmentos capturados dentro y fuera de la intranet? ¿Se está modificando el contenido de los mensajes, como en el caso de **ftp**?