Práctica 5: NAT: funcionamiento y análisis de trazas

1. Sesión L5

Lectura previa: Kurose 4.4.2 subapartado “Traducción de direcciones de red” (pags. 339-342)

Trabajo previo antes de la sesión de laboratorio: Introducción (lectura), Traducción de direcciones de red (estudio).

2. 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.

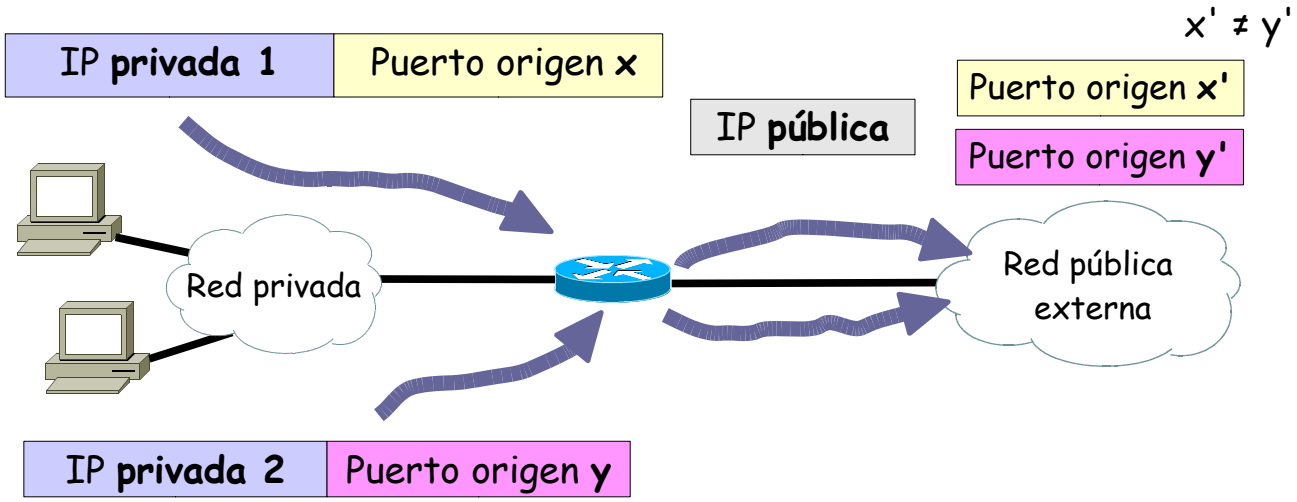
Una mejor opción es seguir contratando una única dirección IP e idear algún mecanismo para compartir esa dirección que nos ha proporcionado el ISP entre los ordenadores de la red de casa o de la oficina. Este mecanismo se conoce como traducción de direcciones, o NAT (Network Address Translation).

3. Traducción de direcciones de red

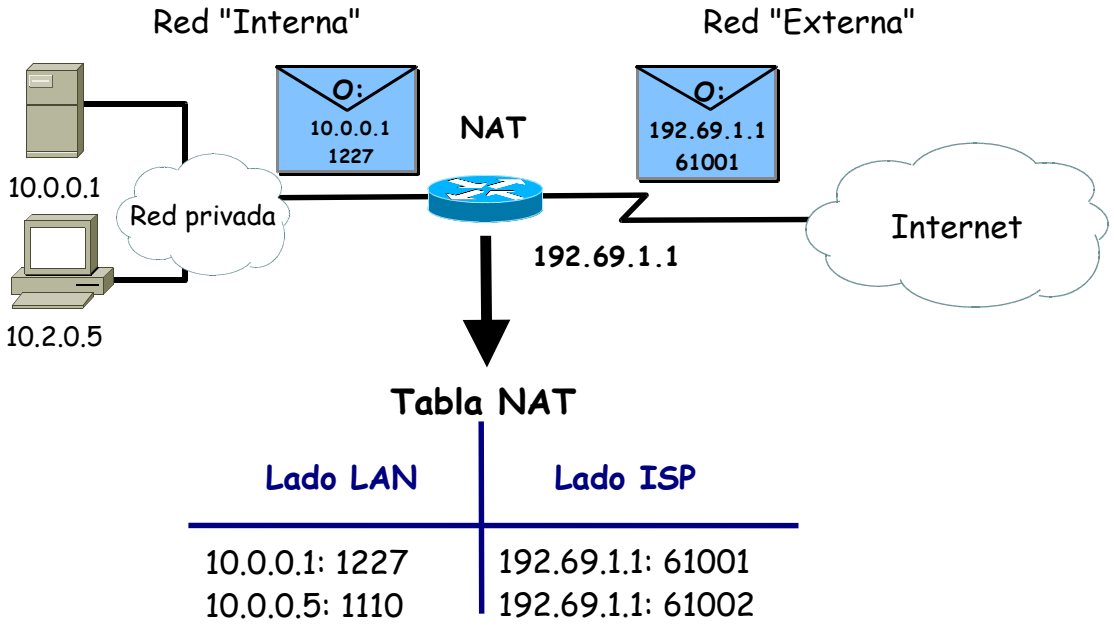
El mecanismo de traducción de direcciones de red (NAT) se complementa generalmente con el uso de direcciones privadas, de forma que es habitual encontrar dicho tipo de direcciones en la red local de casa o de la oficina (también conocida como intranet) que usan este mecanismo para acceder a Internet. 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 4.4.2 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, 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 que tiene la IP 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

a) 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. ¿Por qué nos dice el NAT que la dirección IP de la puerta de enlace es incorrecta? Porque segun la mascara de red su ip y la de la puerta de enlace no estan en la misma red

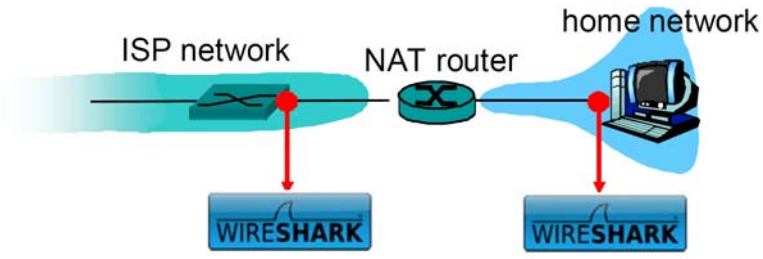
b) Si ambas direcciones IP son correctas, ¿qué parámetro habría que cambiar para que la configuración fuera correcta?¿Qué valor haría correcta la configuración? La mascara de red : 255.255.254.0

c) ¿Pueden estar los DNS en una red distinta a la nuestra? Justifica la respuesta.
Si, porque es un servicio a parte que no hace falta para conectarse a internet.

4. Análisis de tráfico

porque mientras tengas acceso a el, no hace falta que este en la misma red.

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. Abre desde el wireshark el fichero HTTP_LAN_1 y responde a las siguientes cuestiones.

192.168.1.181 158.42.4.23 173.194.34.197

1. ¿Cuál es la dirección IP del cliente? ¿Cuál es la dirección IP del servidor web?
2. ¿Cuántas conexiones TCP se realizan? 2
3. Localiza el datagrama que contiene la petición web “GET / HTTP/1.1”. ¿Cuáles son

los puertos TCP fuente y destino? src: 52467 dst: 80

en el instante 4

4. ¿En qué momento exacto se recibe la correspondiente respuesta HTTP 200 OK desde el servidor web? ¿Cuáles son las direcciones IP fuente y destino del datagrama correspondiente? ¿Y los puertos fuente y destino? src: 158.42.4.23:80 dst: 192.168.1.181:52467

5. ¿Qué puertos se usan en la segunda conexión TCP?
src: 39137 dst 80

Ejercicio 3. Una vez realizado el ejercicio 2, vamos a centrarnos ahora en los mensajes HTTP que salen del router NAT hacia el servidor web. Para ello, desde el programa Wireshark abre el fichero de captura HTTP_ISP_1, que se corresponde con el tráfico del ejercicio 2 anterior, pero en la parte externa del NAT. Cuando estudies esta nueva captura, ten en cuenta que los tiempos de las tramas no se corresponden con precisión a los del fichero anterior, dado que ambas capturas no están sincronizadas.

en el instante 3

src: 158.42.180.22:52467
dst: 158.42.4.23:80
la ip fuente es diferente

1. En este nuevo fichero de captura, localiza el primer mensaje HTTP GET que se envió, en la captura anterior del ejercicio2, desde el cliente al servidor web en el instante 1.338012. ¿En qué momento aparece este mensaje en el fichero HTTP_ISP_1? ¿Cuáles son las direcciones IP fuente y destino y los puertos que se usan? ¿Cuáles de estos campos son los mismos y cuales diferentes que en el caso del fichero anterior?

2. ¿Cuál es la direccion IP pública del router NAT? 158.42.180.22

Se ha cambiado la ip fuente ahora es la del NAT para poder utilizar una ip publica

3. ¿Se ha cambiado algún campo del mensaje HTTP GET? ¿Y del datagrama IP que contiene dicho mensaje? Para aquellos campos que se han modificado ¿cuál es el motivo?

src: 158.42.4.23
dst: 158.42.180.22
No son iguales

4. En el fichero HTTP_ISP_1, ¿en qué momento se recibe desde el servidor web el mensaje HTTP 200 OK? ¿Cuáles son las direcciones IP fuente y destino del datagrama? ¿Son iguales a las que has analizado en el ejercicio anterior?

en el instante 4

Ejercicio 4. Basándote en la información que has recogido, rellena la tabla de traducciones siguiente:

Lado red local		Lado ISP	
Dirección IP origen	Puerto origen	Dirección IP origen	Puerto origen
192.168.1.181	52467	158.42.180.22	52467
192.168.1.181	39137	158.42.180.22	39137

Comprueba también las direcciones IP destino.

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 UnknownHostException, IOException {


   String mi_IP =  "192.168.1.2";
   Socket s = new Socket("www.redes.upv.es",80, InetAddress.getByName(mi_IP), 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);
}}
```

Obviamente, 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 un 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 con el Wireshark el fichero HTTP_LAN_2, que corresponde al tráfico generado por uno de los ordenadores de la red privada donde se ha ejecutado el programa anterior.

1. ¿Cuál es la dirección IP del cliente? ¿Cuál es la dirección IP del servidor web? 192.168.1.2 158.42.53.72
2. ¿Cuáles son los puertos TCP fuente y destino? src: 40000 dst: 80

Abre el fichero HTTP_ISP_2. Este fichero contiene el tráfico generado en la red pública por los dos ordenadores de la red privada. La primera conexión al servidor web usa el mismo número de puerto origen que en el lado LAN, pero en la segunda conexión TCP ...

1. ¿Qué número de puerto origen asigna el router NAT? 40016
2. ¿Cómo se puede saber cuál de la dos conexiones TCP corresponde a la contenida en el fichero HTTP_LAN_2? Sugerencia: revisa identificador del paquete IP. la segunda conexion

Basándote en la información que has recogido, rellena la tabla de traducciones siguiente:

Lado red local		Lado ISP	
Dirección IP origen	Puerto origen	Dirección IP origen	Puerto origen
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. ¿Cuál es la dirección IP del cliente? 192.168.1.2 ¿Cuál es la dirección IP del servidor ftp? 158.42.180.62
2. ¿Cuántas conexiones TCP aparecen? src1: 40831 dst1: 21 src2: 45162 dst2: 20 ¿Cuáles son los puertos TCP fuente y destino de cada una de ellas? ¿Por qué hay varias conexiones TCP?
3. Fíjate en el datagrama que se genera en la red privada en el instante 4.307125. Comparalo con el correspondiente de la red externa. Analiza también los segmentos de fin de la conexión que hay al final de las capturas, tanto en la parte LAN como en la parte del ISP. ¿Qué está sucediendo? En caso de duda, pregunta a tu profesor de prácticas.

5. Servidores dentro de la intranet

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.

Sin embargo, habilitar un servidor dentro de la intranet de forma que pueda ser accedido desde el exterior requiere un poco más de trabajo. La razón es que el funcionamiento normal del NAT es que cuando llega un datagrama desde el exterior, el NAT busca en la tabla de traducciones la equivalencia a usar para deshacer los cambios previos. No obstante, cuando se trata de acceder desde al exterior a un servidor en la intranet, todavía no existe esa equivalencia y por tanto el router NAT no sabe qué transformaciones debe realizar. Por tanto, hay que "enseñarle" al router NAT lo que debe hacer con esas 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 las direcciones IP de la intranet se asignan dinámicamente gracias al servidor DHCP habitualmente 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 al puerto del servidor, el router la reenviará a la dirección IP de la intranet que tenga configurada, pero el servidor ya no estará 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.

158.42.180.21 192.168.1.2

1. ¿Cuál es la dirección IP del cliente? ¿Cuál es la dirección IP del servidor ssh?
2. ¿Cuáles son los puertos TCP fuente y destino? src: 44628 dst: 22
3. ¿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?

Solo cambia la ip destino, No se modifica el contenido del mensage