0.1 NAT para IPv4

El término NAT es la abreviatura de *Network Address Transalation* o direcciones de red. NAT es el proceso mediante el cual una o más direcciones locales (*local address*) se traducen en una más direcciones globales (*global IP address*) y viceversa, con el fin de proporcionar acceso a internet a los host locales.
Además de esto el NAT es el encargado de sustituir la red privada o *private network* por la IP pública del router, con el objetivo de facilitar el acceso a internet de los nodos en direcciones privadas, haciendo que los direccionamientos sean compatibles. Este router mantiene una tabla de conexiones para saber luego a quién se debe enviar los datos.
Este puede ser el caso de tu red doméstica y la red de Internet, siendo necesario el modo NAT para que puedas llegar a conectar a la red global y así recibir o enviar información a ella. Si lo has pensado, la mayoría de usuarios tenemos las mismas direcciones IP dentro de nuestra casa, las típicas 192.168.1.xxx, o las que nosotros decidamos configurar en el router en un momento dado. Entonces te preguntas: si son las mismas IP ¿por qué el paquete de datos no le llega al vecino en lugar de a mí?
Podemos decir que en vez de tener que asignar una dirección IP diferente para cada de los dispositivos conectados, el NAT lo que hace es dar una única para todos. Puede ser cualquiera entre 192.168.0.0 y 192.168.255.255. Los paquetes de datos que proceden de Internet contienen la dirección IPv4 externa en su encabezado. Según el tipo de datos, el NAT lo reenvía a los dispositivos privados o internos para que los datos puedan procesarse según sea necesario.
Pues aquí es donde actúa el NAT, ya que oculta todo el espacio de direcciones IP privadas detrás de una sola dirección IP, o unas cuantas en función del modo NAT que se utilice. Esta sería la dirección IP pública del router, la que realmente conecta nuestra red interna a la red externa. Cuando el paquete de información llega a nuestro router, realmente lo ha hecho al tener información sobre esa IP pública. Será por tanto el router el que analice el paquete y compruebe si efectivamente hay un destinatario dentro de su red que está pidiendo esta información y la dejará entrar.

0.1.1 Tipos de NAT

1. **NAT estática**: Este tipo de NAT, normalmente es utilizada cuando la dirección local es convertida a su vez en una dirección pública, lo que esto quiere decir es que, habrá una dirección IP asociada a nuestro router o dispositivo NAT que será consistente.
2. **NAT dinámica**: En este caso la dirección IP privada se traduce a una IP pública de una lista que tenga el router. De esta forma cuando una determinada IP privada quiere acceder al exterior, el router comprueba en su lista propia cuál es la IP pública que está libre para asignársela. Esto añade mayor seguridad para los hosts que pertenezcan a esa red privada, ya que permite enmascarar la configuración interna de la red la ser IP asignadas aleatoriamente. Lo que sí debe asegurarse en este modo NAT es que todos los host, al menos puedan tener una IP pública asociada en el caso de que todos ellos se conecten a la vez.
3. **NAT por sobrecarga**: El último quizás sea el más importante o útil en lo que se refiere a nuestra red privada doméstica, ya que es el modo NAT que usa nuestro router. Sin duda el más utilizado por utilizar también puertos, además de IP para la traducción. Por ello recibe también el nombre de Port Address Translation o PAT.
   En este caso, nuestro router solamente tiene asignada una dirección pública a la vez,

y esta incluso puede ser dinámica al asignarse por DHCP cuando el router se arranca. En teoría, un router podría coger una IP pública distinta cada vez que se encendiera. Pero en la práctica, se asignará casi siempre la misma IP por estar ya asociada al router con anterioridad mediante la MAC. Es exactamente lo que ocurre cuando un router le asigna la misma IP a nuestro PC cada vez que se enciende.

Vamos a explicarlo a la siguiente manera[1]

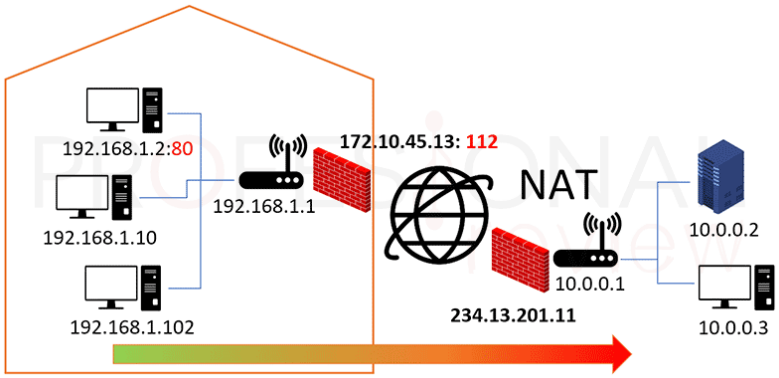

Figure 1: Red privada a pública

Este modo NAT de sobrecarga permite comunicarnos con el exterior **sin desvelar** la IP privada que tiene nuestro equipo. Esto lo hace a través de una **IP pública** que tiene asignada el router para salir a Internet, es todo bastante intuitivo.

Imaginemos que subimos una foto a Instagram desde nuestro equipo, para ello nos tenemos que conectar a la IP del servidor a donde se guardará la foto. Nuestro PC tiene la **dirección privada 10.0.0.3**, y se pone en contacto con el router para enviar el paquete.

Este paquete además tiene asociado un número de puerto de origen, por ejemplo el 80 si estamos en nuestro navegador. A continuación, el router detecta que nuestro equipo desea comunicarse con una remota perteneciente a Internet, así que coge el paquete y le reasigna la dirección IP pública de nuestra conexión y un puerto escogido al azar de entre los 65.536 que hay disponibles y que no esté en uso.

Finalmente el paquete se envía a la red de Internet hasta llegar a la IP pública del otro extremo. Dependiendo del modo NAT que utilice, hará un proceso de traducción similar de IP y de puerto para almacenar la foto en uno de los servidores (con su IP privada) que haya detrás de la IP pública de Instagram.

[1]Ejemplo sacado de *Profesional review* https://www.profesionalreview.com/2020/08/22/modo-nat-que-es/Que_es_el_modo_NAT

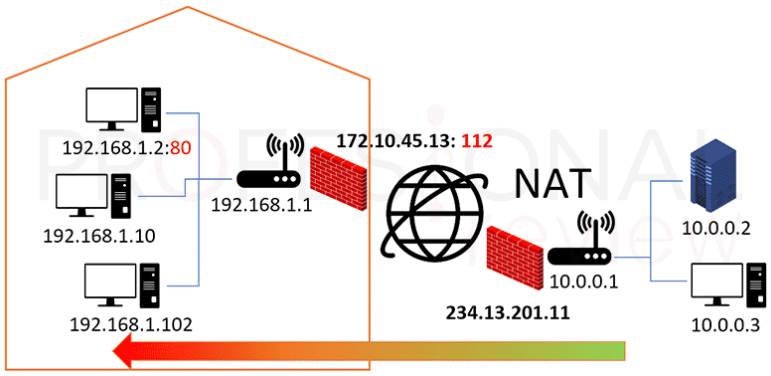

Figure 2: Red privada a pública

El proceso contrario será el mismo, cuando un paquete llega a nuestro router a través de una dirección IP y un puerto al azar, este analiza si el paquete va destinado a algún nodo de su red interna mediante la información de la cabecera. Si es así, cambiará de nuevo al puerto al que corresponda, por ejemplo el 80 si debe verse en el navegador, y la dirección IP de destino a la IP interna de nuestro PC. De esta forma, el proceso concluye.

0.1.2 Ventajas y desventajas

Ventajas:

- Conserva los esquemas y rangos de direccionamiento registrados legalmente, permitiendo así la privatización de intranets, como sabemos, el surgimiento del NAT fue para ahorrar en uso de direcciones IP públicas, ya que estas tenían un número limitado.
- Conserva las direcciones a través de la multiplexación de aplicaciones a nivel de puertos, esto se utiliza en la mayoría de casos en los que se utiliza PAT (Traducción de la dirección del puerto) por sus siglas en inglés, y en el cual podemos realizar el manejo de múltiples equipos y/o aplicaciones utilizando una sola dirección IP gracias a la utilización de los puertos TCP y UDP.
- Aumenta la flexibilidad de las conexiones a las redes públicas, esto quiere decir que podemos mantener nuestro direccionamiento privado IPv4 y al mismo tiempo permite mantener los cambios a nuevas direcciones públicas.
- Permite ocultar las direcciones IPv4 privadas de los usuarios y otros dispositivos, esto significa que, al momento de la traducción de direcciones, el usuario tendrá una dirección privada y a su vez una dirección pública diferente a esa dirección privada evitando que esta sea conocida.

Desventajas:

- Se deteriora el rendimiento de la red, en especial, en el caso de los protocolos en tiempo real como VoIP. NAT aumenta los retrasos de reenvió porque la traducción de cada dirección IPv4 dentro de los encabezados de los paquetes lleva tiempo.
- Se pierde el direccionamiento de extremo a extremo. Muchos protocolos y aplicaciones de Internet dependen del direccionamiento de extremo a extremo desde el origen hasta el destino. Algunas aplicaciones no funcionan con NAT. Por ejemplo, algunas aplicaciones de seguridad, como las firmas digitales, fallan porque la dirección IPv4 de origen cambia antes de llegar a destino. Las aplicaciones que utilizan direcciones físicas, en lugar de un nombre de dominio calificado, no llegan a los

destinos que se traducen a través del router NAT. En ocasiones, este problema se puede evitar al implementar las asignaciones de NAT estática.
- Se reduce el seguimiento IPv4 de extremo a extremo. El seguimiento de los paquetes que pasan por varios cambios de dirección a través de varios saltos de NAT se torna mucho más difícil y, en consecuencia, dificulta la resolución de problemas.
- Genera complicaciones en la utilización de protocolos de tunneling, como IPsec, porque NAT modifica valores en los encabezados, lo que hace fallar las comprobaciones de integridad.
- El inicio de las conexiones TCP puede interrumpirse. A menos que el router NAT esté configurado para admitir dichos protocolos, los paquetes entrantes no pueden llegar a su destino. Algunos protocolos pueden admitir una instancia de NAT entre los hosts participantes (por ejemplo, FTP de modo pasivo), pero fallan cuando NAT separa a ambos sistemas de Internet.

0.1.3 Configurar

0.1.3.1 NAT estática

La configuración estática de una NAT se divide en una relación de 1 a 1, una dirección IP privada a una dirección IP pública. Por lo que existe una traducción en la tabla de direcciones de la NAT tan pronto como se configura con los comandos NAT, siendo posible borrarlos únicamente con los mismos comandos. Para configurar la NAT estática en el software Packet Tracer de cisco, accedemos al modo de configuración global del Router e introducimos el siguiente comando:

```
R1(config)# ip nat inside source static [direccion privada]
   [direccion global]
```

Luego configuramos las interfaces del router que tienen la direccion privada y global

```
R1(config)# interface gi 0/0/0
R1(config-int)# ip nat inside
R1(config-int)# interface gi 0/0/1
R1(config-int)# ip nat outside
```

0.1.3.2 NAT dinámica

Por otro lado tenemos la configuración de la NAT dinámica, la cual se encarga de que las direcciones IP privadas pertenecientes a una red tengan acceso a otras redes por medio de un conjunto de direcciones de IP pública, las cuales se asignan a cada host de forma aleatoria.
Para configurar la NAT dinámica en CPT, primeramente ingresamos al modo de configuración global del router. Luego creamos una conjunto de direcciones IP públicas por las cuales accederemos a otras redes

```
R1(config)# ip nat pool [nombre] [conjunto de direcciones
   públicas] netmask [máscara de la red]
```

Posteriormente configuramos una lista de acceso, la cual contendrá las direcciones de nuestra red privada

```
R1(config)# access-list [N#] permit [dirección de red] [máscara
   invertida]
```

Finalmente, configuramos las interfaces del router que contendrán la red privada y la red global.

```
ip nat inside source static {local-ip} {local-port} {global-ip}
   {global port}
```

Para traducir 192.168.1.1 a 192.168.2.200

```
R1(config)#ip nat inside source static 192.168.1.1 192.168.2.200
```