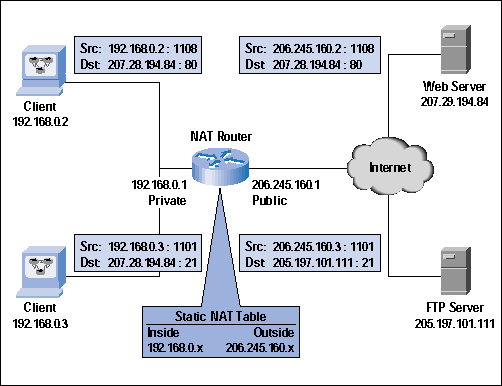
# CAPA DE RED

## ¿Qué es el NAT?

### Definición

La traducción de direcciones de red o NAT (del inglés Network Address Translation) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.



* 1. **Cómo pueden influir en la programación de comunicación en red**
  2. **Qué tipos hay según influyan en esta comunicación**
* **NAT de cono completo (Full-Cone NAT).** En este caso de comunicación completa, NAT mapeará la dirección IP y puerto interno a una dirección y puerto público diferentes. Una vez establecido, cualquier host externo puede comunicarse con el host de la red privada enviando los paquetes a una dirección IP y puerto externo que haya sido mapeado. Esta implementación NAT es la menos segura, puesto que una atacante puede adivinar qué puerto está abierto.
* **NAT de cono restringido (Restricted Cone NAT).** En este caso de la conexión restringida, la IP y puerto externos de NAT son abiertos cuando el host de la red privada quiere comunicarse con una dirección IP específica fuera de su red. La NAT bloqueará todo tráfico que no venga de esa dirección IP específica.
* **NAT de cono restringido de puertos (Port-Restricted Cone NAT).** En una conexión restringida por puerto NAT bloqueará todo el tráfico a menos que el host de la red privada haya enviado previamente tráfico a una IP y puerto especifico, entonces solo en ese caso ésa IP:puerto tendrán acceso a la red privada.
* **NAT Simétrica (Symmetric NAT).** En este caso la traducción de dirección IP privada a dirección IP pública depende de la dirección IP de destino donde se quiere enviar el tráfico.

## ¿Qué implicaciones tiene para comunicaciones TCP?

### Ventajas / Desventajas

#### Ventajas de la NAT

* El gran ahorro de direcciones IPv4 que supone, recordemos que podemos conectar múltiples máquinas de una red a Internet usando una única dirección IP pública.
* Las máquinas conectadas a la red mediante NAT no son visibles desde el exterior, por lo que un atacante externo no podría averiguar si una máquina está conectada o no a la red.
* Mantenimiento de la red. Sólo sería necesario modificar la tabla de reenvío de un router para desviar todo el tráfico hacia otra máquina mientras se llevan a cabo tareas de mantenimiento.

#### Desventajas de la NAT

La NAT es solo un parche, no una solución al verdadero problema, por tanto también tiene una serie de desventajas asociadas a su uso:

* Checksums TCP y UDP: El router tiene que volver a calcular el checksum de cada paquete que modifica. Por lo que se necesita mayor potencia de computación.
* No todas las aplicaciones y protocolos son compatibles con NAT. Hay protocolos que introducen el puerto de origen dentro de la zona de datos de un paquete, por lo que el router no lo modifica y la aplicación no funciona correctamente.

### Soluciones al NAT

Una posible solución que puede evitar el uso de la NAT seria la implementación de IPv6 que es una versión del Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791, que a 2016 se está implementando en la gran mayoría de dispositivos que acceden a Internet.

IPv4 posibilita 4 294 967 296 (232) direcciones de host diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada dispositivo, teléfono, PDA, táblet, etcétera. En cambio, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2128 o 340 sextillones de direcciones) —cerca de 6,7 × 1017 (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la Tierra.

**Fuentes:**

* **Ventajas/desventajas**: <https://www.xatakamovil.com/conectividad/nat-network-address-translation-que-es-y-como-funciona>
* **NAT y tipos :** <https://es.wikipedia.org/wiki/Traducci%C3%B3n_de_direcciones_de_red#Tipos_de_NAT>
* **IPv6:** <https://es.wikipedia.org/wiki/IPv6>
* **Imagen:** <https://www.cisco.com/c/dam/en_us/about/ac123/ac147/downloads/customer/internetprotocoljournal/ipj_3-4/images/Fig21.gif>