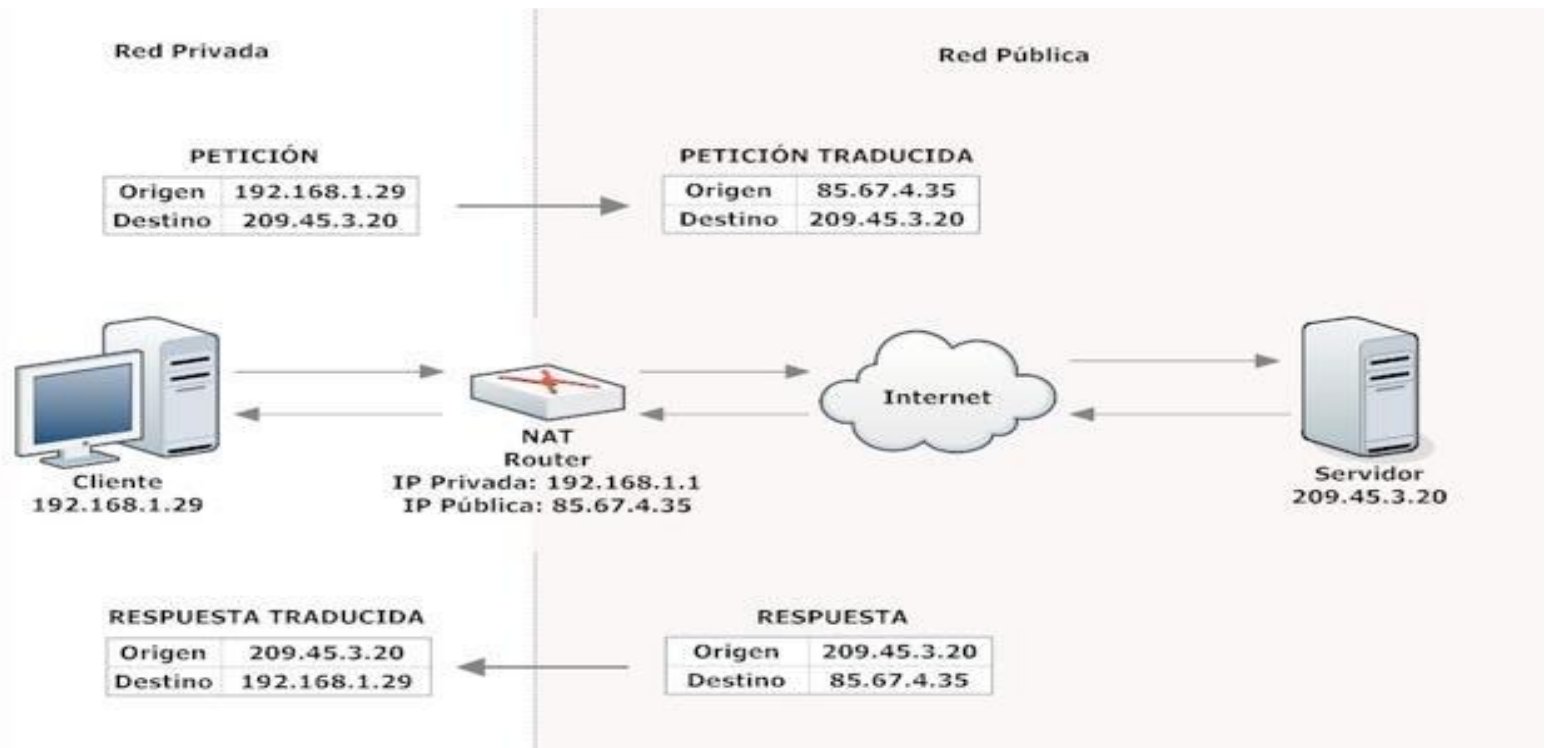


NAT

¿Qué es NAT?

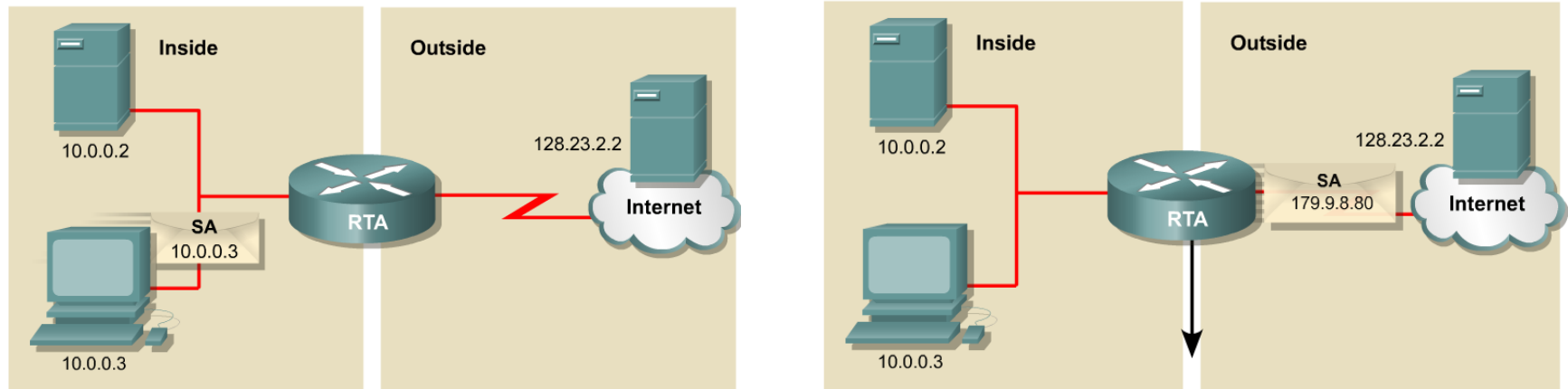
- NAT (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.



Funcionamiento

- El protocolo TCP/IP tiene la capacidad de generar varias conexiones simultáneas con un dispositivo remoto. Para realizar esto, dentro de la cabecera de un paquete IP, existen campos en los que se indica la dirección origen y destino. Esta combinación de números define una única conexión
- La mayoría de los NAT asignan varias máquinas (hosts) privadas a una dirección IP expuesta públicamente. En una configuración típica, una red local utiliza unas direcciones IP designadas “privadas” para subredes (RFC 1918). El router está conectado a Internet por medio de una dirección pública asignada por un proveedor de servicios de Internet. Como el tráfico pasa desde la red local a Internet, la dirección de origen en cada paquete se traduce sobre la marcha, de una dirección privada a una dirección pública. El router mantiene los datos básicos de cada conexión activa (en particular, la dirección de destino y el puerto). Cuando una respuesta llega al router utiliza los datos de seguimiento de la conexión almacenados en la fase de salida para determinar la dirección privada de la red interna a la que remitir la respuesta.

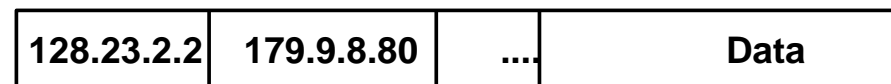
Ejemplo NAT



NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.3	179.9.8.80	128.23.2.2

DA SA

DA SA



IP Header

IP Header

NAT 1 a 1

- Conocida también como NAT estática, Consiste básicamente en un tipo de NAT en el cuál se mapea una dirección IP privada con una dirección IP pública de forma estática. De esta manera, cada equipo en la red privada debe tener su correspondiente IP pública asignada para poder acceder a Internet. La principal desventaja de este esquema es que por cada equipo que se desee tenga acceso a Internet se debe contratar una IP pública. Además, es posible que haya direcciones IP públicas sin usar (porque los equipos que las tienen asignadas están apagados, por ejemplo), mientras que hay equipos que no puedan tener acceso a Internet (porque no tienen ninguna IP pública mapeada).

NAT 1 a muchos

- También conocido como NAT Dinámico, este tipo de NAT pretende mejorar varios aspectos del NAT estático dado que utiliza un pool de IPs públicas para un pool de IPs privadas que serán mapeadas de forma dinámica y a demanda. La ventaja de este esquema es que si se tienen por ejemplo 5 IPs públicas y 10 máquinas en la red privada, las primeras 5 máquinas en conectarse tendrán acceso a Internet. Si suponemos que no más de 5 máquinas estarán encendidas de forma simultánea nos garantiza que todas las máquinas de nuestra red privada tendrán salida a Internet eventualmente.

PAT

- El caso de NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos y el más usado en los hogares. Consiste en utilizar una única dirección IP pública para mapear múltiples direcciones IPs privadas. Las ventajas que brinda tienen dos enfoques: por un lado, el cliente necesita contratar una sola dirección IP pública para que las máquinas de su red tengan acceso a Internet, lo que supone un importante ahorro económico; por otro lado se ahorra un número importante de IPs públicas, lo que demora el agotamiento de las mismas.

La pregunta casi obvia es cómo puede ser que con una única dirección IP pública se mapeen múltiples IPs privadas. Bien, como su nombre lo indica, PAT hace uso de múltiples puertos para manejar las conexiones de cada host interno. Veamos esto con el siguiente ejemplo:

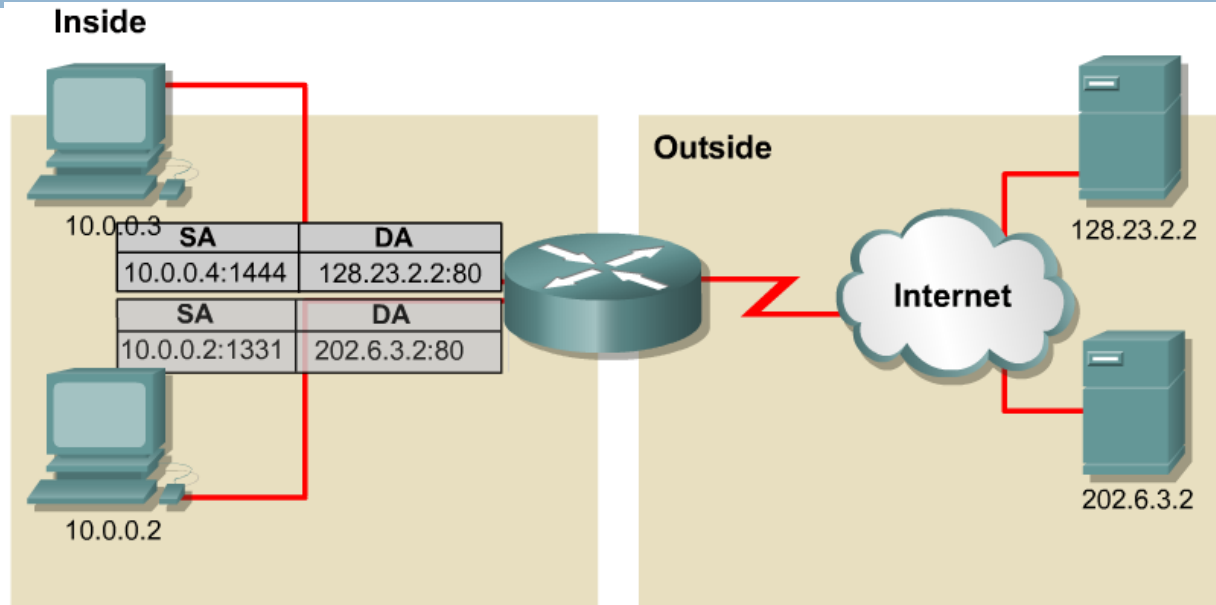
La PCA quiere acceder a www.netstorming.com.ar. El socket está formado por:

- IP origen: PCA.
- Puerto origen: X.
- IP destino: www.netstorming.com.ar.
- Puerto destino: 80.

Al llegar el requerimiento anterior al router que hace PAT, el mismo modifica dicha información por la siguiente:

- IP origen: router.
- Puerto origen: Y.
- IP destino: www.netstorming.com.ar.
- Puerto destino: 80.
- Además, el router arma una tabla que le permite saber a qué máquina de la red interna debe dirigir la respuesta. De esta manera, cuando recibe un segmento desde el puerto 80 de www.netstorming.com.ar dirigido al puerto Y del router, este sabe que debe redirigir dicha información al puerto X de la PCA.

Ejemplo PAT



NAT Table			
Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global Address
10.0.0.2:1331	179.9.8.20:1331	202.6.3.2:80	202.6.3.2:80
10.0.0.3:1555	179.9.8.20:1555	128.23.2.2:80	128.23.2.2:80

Port Forwarding

- Es usado en el sentido opuesto. Por ejemplo si tienes un servidor web corriendo en la computadora de tu casa, nadie en internet tiene acceso al mismo. Tu servidor web al igual que tu computadora tendrán una dirección IP privada (no ruteable en Internet). Pero se podría crear una política en el router que diga que todo tráfico originado en el internet destino a la interfaz pública del router con el puerto 80 debería ser enviado a la dirección 192.168.1.x del Web server.

Basicamente, port forwarding permite a la gente de internet acceder a servicios en una red privada. Si la red privada tiene direcciones públicas, entonces no se necesitaría port forwarding. El servidor web sería accesible directamente a través de su dirección de IP Pública.

Ejemplos de Software de NAT

- Internet Connection Sharing (ICS): NAT+DHCP para Windows desde W98SE
- WinGate: como ICS pero con más control
- IPFilter: Solaris, NetBSD, FreeBSD, xMach.
- PF (software): El filtro de paquetes OpenBSD.
- Netfilter/iptables el filtro de paquetes de Linux y su interface

Ejemplos de Configuración

- Ejemplificaremos como debe ser la configuración de NAT estático, NAT dinámico y NATP/PAT en ese orden en CISCO.

Configuracion de NAT estatico

- Para configurar este tipo de NAT en Cisco nos valemos de los siguientes comandos, donde se ve que el equipo con IP 192.168.1.6 conectado por medio de la interfaz fastEthernet 0/0 será nateado con la IP pública 200.41.58.112 por medio de la interfaz de salida serial 0/0.
- Router(config)# ip nat inside source static 192.168.1.6 200.41.58.112
Router(config)# interface fastEthernet 0/0
Router(config-if)# ip nat inside
Router(config)# interface serial 0/0
Router(config-if)# ip nat outside

Configuracion de NAT dinamico

- Para configurar este tipo de NAT definimos el pool de IPs públicas disponibles y el rango de direcciones privadas que deseamos que sean mapeadas.

En el siguiente ejemplo se cuenta con las direcciones IPs públicas desde la 163.10.90.2 a la 163.10.90.6 y la subred privada 192.168.1.0/24.

- Router(config)# ip nat pool name DIR_NAT_GLOB 163.10.90.2 163.10.90.6 netmask 255.255.255.240

Router(config)# access-list 10 permit 192.168.1.0 0.0.0.255

Router(config)# ip nat inside source list 10 pool DIR_NAT_GLOB

Router(config)# interface fastEthernet 0/0

Router(config-if)# ip nat inside

Router(config)# interface serial 0/0

Router(config-if)# ip nat outside

Configuracion NATP/PAT(NAT overload)

- La forma de configurar NAT con sobrecarga es la siguiente:
- Router(config)# access-list 10 permit ip 192.168.146.0 0.0.1.255
Router(config)# ip nat inside source list 10 interface serial 0/0 overload
Router(config)# interface fastEthernet 0/0
Router(config-if)# ip nat inside
Router(config)# interface serial 0/0
Router(config-if)# ip nat outside
- El primer comando es para permitir acceso a dispositivos con ip en rango 192.168.146.0 a 192.168.147.254.
- El segundo comando es para habilitar NAT overload en base a la lista configurada anteriormente
- El tercero y cuarto comando son para poner la interfaz fastEthernet 0/0 como interfaz interna.
- El quinto y sexto comando son para poner la interfaz serial S0/0 como interfaz externa.

Y ahora práctica en Linux...

Usando la herramienta iptables

NAT Estático con iptables

- ❑ `iptables -t nat -A PREROUTING -d 192.168.0.1 -j DNAT --to-destination 10.0.2.15`
- ❑ `iptables -t nat -A POSTROUTING -d 10.0.2.15 -j SNAT --to-source 200.10.1.2`

NAT Dinámico con iptables

- # Restringido por mascara
- `iptables -t nat -A POSTROUTING -o eth0 -s 10.0.2.0/24 -j SNAT --to-source 192.168.0.0/24`
- # Restringido para un rango de IPs especifico
- `iptables -t nat -A POSTROUTING -o eth0 -s 10.0.2.1-10.0.2.15 -j SNAT --to-source 192.168.0.1-15`

NAT Dinámico con Overload (IP Masquerading)

- # Para IPs variables
- `iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`

- # Para IPs estaticas
- `iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 200.10.1.2`

- # Con restricciones de IPs de origen
- `iptables -t nat -A POSTROUTING -o eth0 -s 192.168.0.0/24 -j SNAT --to-source 200.10.1.2`

IETF standards documents (RFCs)

- **The IP Network Address Translator (NAT) » RFC 1631**
- **IP Network Address Translator (NAT) Terminology and Considerations » RFC 2663**
- **Traductor de Dirección de Red IP Tradicional (NAT Tradicional)» RFC 3022**
- **Address Allocation for Private Internets » RFC 1918**

Referencias

- Computer Networks –Andrew S. Tanenbaum
- <https://www.ietf.org/rfc>
- <http://es.wikipedia.org/>
- <http://www.monografias.com/>
- <https://learningnetwork.cisco.com/>
- <http://searchnetworking.techtarget.com/>
- <http://www.adslfaqs.com.ar/>
- <http://publib.boulder.ibm.com/>
- <http://www.mikroways.net/>
- <http://www.tp-link.com/>
- <http://www.firewall.cx/>