

NAT: Linux, Windows y Cisco



IES Gonzalo Nazareno
CONSEJERÍA DE EDUCACIÓN

José Domingo Muñoz
Raúl Ruíz Padilla

Redes de Área Local

Abril 2014

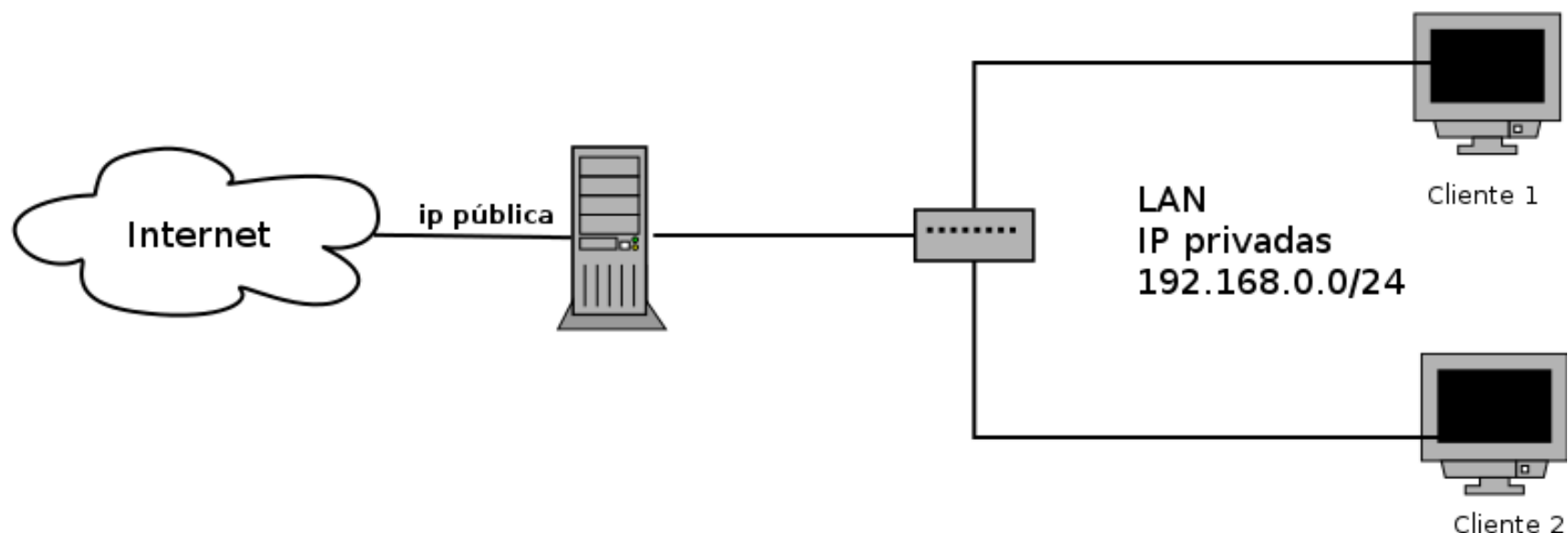
NAT

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.

Existen varios tipos, nosotros vamos a estudiar:

- SNAT (Source NAT) (o PAT, o NAT híbrido): Se cambia la ip de origen con la ip pública del router. Nos permite que varios equipos con ip privadas puedan salir de la LAN usando la ip pública del router.
- DNAT (Destination NAT): Se cambia la ip de destino, nos permite que en un equipo externo a nuestra red pueda acceder a los servidores de mi red local.

SNAT en Linux



Tenemos un servidor Linux, que realiza dos funciones: hace de router y hace NAT, es decir, cuando un ordenador de la LAN quiere conectar a internet:

- Deja pasar los paquetes de la interfaz conectada a la red privada a la interfaz conecta a internet.
- Cambia la dirección de origen del paquete (ip privada) por la ip pública.

Necesitamos por lo tanto dos tarjetas de red.

SNAT en Linux

Para que la máquina Linux actúe como router tenemos que activar el bit de forward:

1) Escribimos:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```


2) sysctl

De forma alternativa podemos utilizar sysctl, que permite configurar parámetros del kernel mientras se ejecuta:

```
sysctl net.ipv4.ip_forward=1
```

3) /etc/sysctl.conf

Los dos métodos anteriores son equivalentes pero no permanecen tras un reinicio del equipo, para que este cambio se efectúe cada vez que se arranca el equipo editamos el fichero `/etc/sysctl.conf`, buscamos la línea `net.ipv4.ip_forward=1` y la descomentamos.



SNAT en Linux

Para conseguir que la máquina linux haga SNAT tenemos que utilizar
IPTABLES:

En el fichero de configuración de red /etc/network/interfaces podemos añadir
las reglas de iptables

Tenemos dos opciones:

1) Si la ip pública es estática:


```
up iptables -t nat -A POSTROUTING -s <Dir. red local> -o <interfaz ip pública> -j  
SNAT --to <ip pública>
```

```
down iptables -t nat -D POSTROUTING -s <Dir. red local> -o <interfaz ip pública> -j  
SNAT --to <ip pública>
```

Ejemplo:

```
up iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to 192.168.1.15
```

```
down iptables -t nat -D POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to 192.168.1.15
```

A decorative graphic in the bottom right corner consisting of several overlapping, curved green lines that form a stylized, abstract shape, possibly resembling a signal or a leaf.

SNAT en Linux

2) Si la ip pública es dinámica:

```
up iptables -t nat -A POSTROUTING -s <Dir. red local> -o <interfaz ip pública> -j  
MASQUERADE
```

```
down iptables -t nat -D POSTROUTING -s <Dir. red local> -o <interfaz ip pública> -j  
MASQUERADE
```

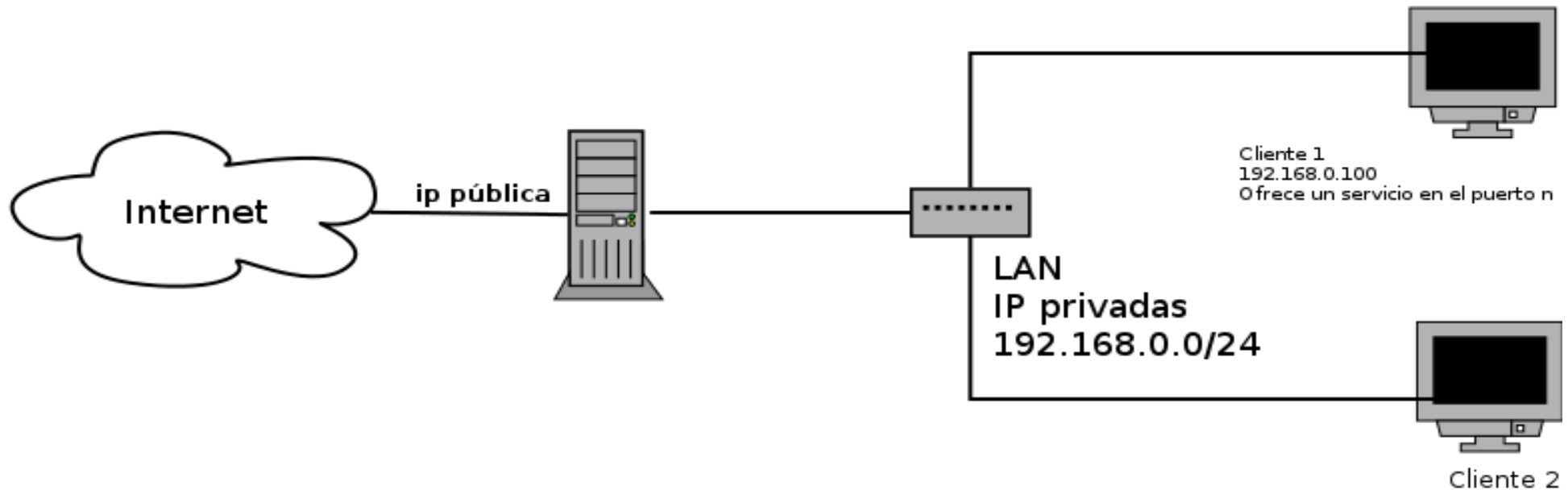
Ejemplo:

```
up iptables -t nat -A POSTROUTING -o eth0 -s 192.168.1.0/24 -j MASQUERADE
```

```
down iptables -t nat -D POSTROUTING -o eth0 -s 192.168.1.0/24 -j MASQUERADE
```



DNAT en Linux



En este caso queremos que una máquina de internet acceda al servicio que ofrece una máquina de nuestra red local por el puerto n . Para ello:

- La máquina externa debe acceder a la ip pública en el puerto n .
- El router debe cambiar la ip de destino, cambia la ip pública por la ip privada del ordenador que ofrece el servicio.

Ejemplo: Tenemos un servidor Web en nuestra red local por el puerto 80. El equipo externo debe conectarse a la ip pública por el puerto 80 (http://ip_publica).

DNAT en Linux

En el fichero /etc/network/interfaces, tenemos que poner una regla iptable:

```
up iptables -t nat -A PREROUTING -p tcp --dport <puerto> -i  
  <interfaz externa> -j DNAT --to <ip privada>
```

```
down iptables -t nat -D PREROUTING -p tcp --dport <puerto> -i  
  <interfaz externa> -j DNAT --to <ip privada>
```

Ejemplo, servidor web en la máquina 192.168.0.100

```
up iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 -j DNAT --to 192.168.0.100
```

```
down iptables -t nat -D PREROUTING -p tcp --dport 80 -i eth0 -j DNAT --to 192.168.0.100
```



SNAT en Windows Server

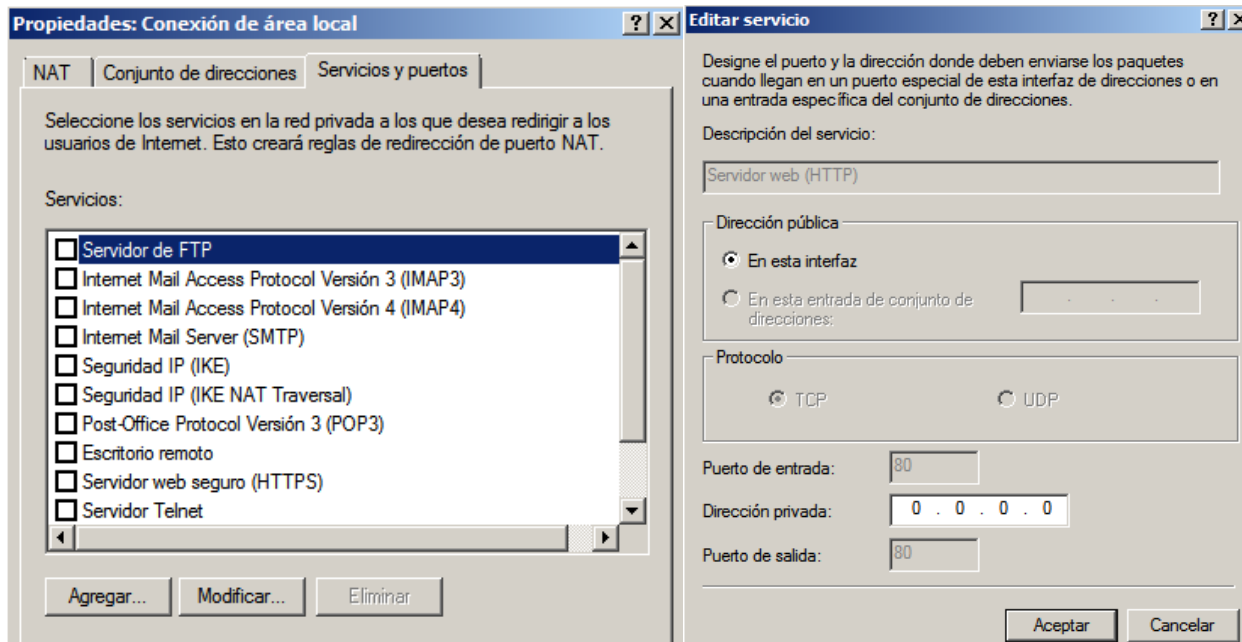
Para que un servidor con Windows Server tenga la función de router y haga NAT:

1. Inicio -> Herramientas administrativas -> Administrador del servidor
2. Agregar roles -> **Servicios de acceso y directiva de redes**
3. En la pantalla servicios de rol escoge **Enrutamiento** -> Instalar
4. En administrador de servidor, en la ventana izquierda, desplegamos la pestaña de Roles, hasta que veamos Enrutamiento y acceso remoto
5. Botón derecho -> Configurar y habilitar Enrutamiento y acceso remoto -> **Traducción de direcciones de red (NAT)** -> Siguiente -> **(Tienes que elegir la interfaz pública)** -> Siguiente -> Configurar más adelante los servicios de nombres y direcciones y direcciones



DNAT en Windows Server

1. Inicio -> Herramientas administrativas -> Enrutamiento y acceso remoto
2. Abre las opciones del servidor → **IPv4 → NAT**
3. Elige las **propiedades** de la interfaz de red que nos da acceso al exterior.
4. En la pestaña **Servicios y puertos** elegimos el servicio deseado (puerto) y la ip privada del equipo que ofrece el servicio.



SNAT en Cisco

1- crear un ACL para definir el tráfico sobre el que se hará NAT

```
router(config)#access-list NUMACL permit IP wilcardmask
```

2- establecer el conjunto de direcciones públicas

```
router(config)#ip nat pool ip_publica IP1 IP2 netmask maskara
```

3- activar nat

```
router(config)#ip nat inside source list NUMACL pool ip_publica overload
```

4. Establecer interfaz interna

```
router(config-if)#ip nat inside
```

5. Establecer interfaz externa

```
router(config-if)#ip nat outside
```



SNAT en Cisco

Comprobar funcionamiento:

```
show ip nat translations
```

```
show ip nat statistics
```

```
debug ip nat
```



SNAT en Cisco

1- crear un ACL para definir el tráfico sobre el que se hará NAT

```
router(config)#access-list NUMACL permit IP wilcardmask
```

2- establecer el conjunto de direcciones públicas

```
router(config)#ip nat pool ip_publica IP1 IP2 netmask maskara
```

3- activar nat

```
router(config)#ip nat inside source list NUMACL pool ip_publica overload
```

4. Establecer interfaz interna

```
router(config-if)#ip nat inside
```

5. Establecer interfaz externa

```
router(config-if)#ip nat outside
```



SNAT en Cisco

1- crear un ACL para definir el tráfico sobre el que se hará NAT

```
router(config)#access-list NUMACL permit IP wilcardmask
```

2- establecer el conjunto de direcciones públicas

```
router(config)#ip nat pool ip_publica IP1 IP2 netmask maskara
```

3- activar nat

```
router(config)#ip nat inside source list NUMACL pool ip_publica overload
```

4. Establecer interfaz interna

```
router(config-if)#ip nat inside
```

5. Establecer interfaz externa

```
router(config-if)#ip nat outside
```



DNAT en Cisco

```
ip nat inside source static tcp ip_privada puerto ip_publica puerto
```

Ejemplo: Tenemos un servidor web en 192.168.1.3 y la ip pública es la 80.59.1.152:

```
ip nat inside source static tcp 192.168.1.3 80 80.59.1.152 80
```

