Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

# Práctica 12 - Network Address Translation (NAT)

## *1- Objetivos*

NAT permite que una red IP parezca hacia el exterior que emplea un espacio de direcciones diferente del que en realidad usa. La utilidad más típica es hacer que una red que emplea direccionamiento privado se pueda conectar a Internet convirtiendo las direcciones IP en los paquetes que envía a direcciones públicas.

En esta práctica vamos a ver conceptos básicos sobre cómo configurar NAT en los routers Cisco.

## *2- Material*

- PCs
- Routers Cisco
- Conmutador
- Hubs

## *3- Avisos generales*

En los ordenadores dispuestos para la realización de estas prácticas (PC A, B y C) se ha creado una cuenta de nombre `lpr` y password `telemat`. Esta cuenta tiene permisos para ejecutar mediante el comando sudo ciertos comandos restringidos normalmente al superusuario. Igualmente se le han otorgado permisos para modificar el contenido de ciertos ficheros del sistema necesarios para la realización de la práctica. Para más detalle diríjanse a la documentación sobre los armarios.

Si quieren conservar cualquier fichero entre sesiones guárdenlo en un disquete o un pendrive, dado que no se asegura que los ficheros creados o modificados durante una sesión de prácticas se mantengan para la siguiente.

Disponen de todos los privilegios en los routers Cisco, es decir, como si fueran el superusuario de un sistema UNIX. En general no tengan miedo de explorar los comandos disponibles en el Cisco IOS, sin embargo, tengan cuidado de no realizar cambios que lo inutilicen. Tengan cuidado con comandos que borren ficheros o sistemas de ficheros. También tengan especial cuidado cuando copien ficheros en la flash dado que puede haber un momento en que el router les pregunte si antes de copiar el fichero desean borrar la flash. **Nunca le digan que sí a que borre la flash** dado que en ella se encuentra el sistema operativo. Si por error proceden a borrar la flash no reinicien ni apaguen el router y avisen al profesor de prácticas. Serán capaces de recuperar este tipo de accidentes cuando aprendan cómo transferir al router ficheros desde un servidor de TFTP.

Al empezar a trabajar con un router tengan cuidado con la configuración que pueda tener grabada y eliminen lo que no necesiten. Antes de abandonar el laboratorio borren de la configuración del arranque sus modificaciones. Para evitar problemas con configuraciones de los routers en sesiones anteriores de prácticas lo primero que deben hacer cuando enciendan el router es borrar el fichero de configuración que carga en el arranque, es decir, en modo privilegiado:

```
Router# erase startup-config
```

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

Una vez hecho esto reinicien el router (comando `reload`). Al terminar de arrancar y no encontrar el fichero de configuración el sistema ejecuta un script (setup) para realizar una primera configuración del router. Salgan del script indicando que no quieren configurar nada. Con eso ya tendrán una configuración en curso limpia (`running-config`). Guárdenla como el nuevo fichero de configuración de arranque:

```
Router# copy running-config startup-config
```

Recuerden: **Nunca le digan que sí a que borre la flash** dado que en ella se encuentra el sistema operativo.

## 4- Introducción a NAT

Un router en el que se haya configurado NAT tendrá normalmente al menos un interfaz en el interior de la red y otro en el exterior. Normalmente se configura NAT en el router de salida de una red. Cuando un paquete está saliendo del dominio, NAT convierte la dirección IP origen en una dirección pública. Cuando un paquete entra en el dominio, NAT convierte la dirección pública destino en el mismo en la dirección local apropiada.

Un router configurado con NAT no anuncia rutas de las redes internas hacia el exterior. Sin embargo, sí puede utilizar la información de enrutado que recibe del exterior.

El Cisco IOS define como el *interior* o *inside* a las redes cuyas direcciones deben ser convertidas. El espacio de direcciones del interior se llama el espacio *local* y el del exterior es el *global*. Las redes a las que se conecta el *interior* se llaman el *exterior* o *outside*.

Veamos las siguientes definiciones:

- Dirección local interior (*Inside local address*): La dirección IP de un host en la red interna cuya dirección probablemente pertenece al rango privado y por lo tanto no puede emplearse en Internet.
- Dirección global interior (*Inside global address*): Una dirección IP pública que representa a una o más direcciones locales.
- Dirección global externa (*Outside global address*): La dirección IP de un host del exterior de la red tal y como ha sido configurado en el exterior.
- Dirección local externa (*Outside local address*): La dirección IP de un host del exterior de la red tal y como aparece en la red interna.

## 5- Conversión estática

Creen la simple topología física de la figura 1.

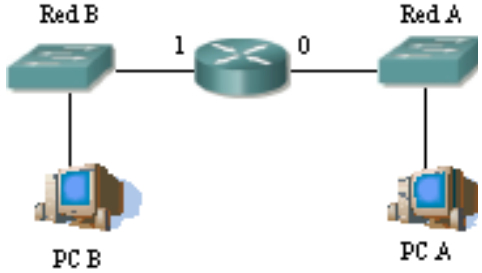


Figura 1.- Dos redes

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

Una de las redes (Red B) representará el *interior* y la otra (Red A) el *exterior*. En el interior emplearemos el espacio de direcciones `192.168.0.0/24`. Para el exterior emplearemos el espacio de direcciones `10.0/16`.

- Asignen dirección a los interfaces del router y a los hosts, así como router por defecto a estos últimos.

Si prueban a hacer ping desde el PC B al PC A debería funcionar. En el caso de que realmente la red interior emplease direccionamiento privado y la red exterior fuera Internet entonces el router no debería reenviar estos paquetes. El router incluiría algún tipo de reglas de filtrado que evitasen este reenvío. En esta asignatura no vamos a ver cómo realizar estos filtrados.

- Dejen ese ping funcionando y pongan un `tcpdump` en PC A para ver los paquetes de ICMP que recibe

Vamos a hacer que el router cambie la direccción del PC B en los paquetes que reenvíe. Para ello:

- Establezcan una regla de conversión estática en modo global de configuración con el comando:

```
Router(config)# ip nat inside source static direccion-local direccion-global
```

En dicho comando `direccion-local` debe ser la dirección IP del PC en la red interior y `direccion-global` la dirección por la que queremos que haga el cambio el router. Escoja una dirección de la red A y tengan en cuenta que ningún otro host en la red exterior puede tener asignada esa dirección.

A continuación debemos especificar qué interfaz está conectado al interior y cuál al exterior.

- Entren en modo configuración del interfaz que esté conectado al interior y ejecuten el comando:

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

- Entren en modo configuración del interfaz que esté conectado al exterior y ejecuten el comando:

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

Verán que desde que ejecutaron este último comando los paquetes ICMP que recibe PC A ya no vienen de la IP real de PC B sino que vienen de la IP global que hemos asignado. Esa IP la hemos escogido de la red externa, es decir, es una IP de la red a la que pertenece PC A. Vean que la cache ARP del router tiene una nueva entrada permanente que corresponde a esa IP global, es decir, hace proxy ARP de ella en la red externa.

Checkpoint 12.1: Muestren al profesor de prácticas que les funciona.

## 6- Conversión dinámica

Ahora vamos a crear un conjunto (*pool*) de direcciones globales que el router empleará para convertir las direcciones internas a ellas.

Primero definiríamos el pool de direcciones públicas disponible:

```
Router(config)# ip nat pool nombre ip-comienzo ip-final netmask mascara
```

Donde `nombre` no es más que un nombre que le damos a este *pool* para poder hacer referencia a él más tarde. Estamos definiendo un rango de direcciones IP, las que vayan desde `ip-comienzo` a `ip-final`. Y finalmente indicamos la máscara de la red a la que pertenecen estas direcciones.

A continuación creamos una lista de acceso con las direcciones de las máquinas a las que convertiremos la dirección IP. No vamos a ver listas de acceso, así que el comando a ejecutar en nuestro caso es:

```
Router(config)# access-list 1 permit 192.168.0.0 0.0.0.255
```

Donde estamos creando la lista de acceso 1 que indica permitir (lo que sea) a las IPs de la red `192.168.0.0` cuyos últimos 8 bits (los que están a 1 en `0.0.0.255`) pueden tener cualquier valor.

Lo siguiente es indicarle que esa lista de acceso contiene las IPs que queremos convertir:

```
Router(config)# ip nat inside source list 1 pool nombre
```

Donde `nombre` es el nombre que hemos dado al *pool*.

Lo único que queda es indicar igual que hicimos antes qué interfaz es el *interior* y cuál el *exterior*.

- Configuren NAT como se acaba de explicar con un pool de sólo 3 direcciones
- Hagan un ping desde PC B a PC A. Pueden ver las conversiones que está haciendo el router con el comando `show ip nat translation`
- Cambien la dirección IP del PC B a otra de la Red B y hagan ping de nuevo (seguramente tendrán que volver a configurar el router por defecto en el PC). Verán una nueva entrada en la tabla de conversiones
- Cambien PC B a otra IP diferente de las anteriores y hagan ping de nuevo. Si cambian a una cuarta IP diferente y hacen ping verán que no funciona, el router ha agotado el pool de direcciones.

Las entradas dinámicas en el pool de direcciones caducan tras cierto periodo de inactividad. El problema es que dicho periodo está configurado por defecto a 24h, pero se puede modificar.

- Detengan los pings
- Borren la tabla de conversiones del router con el comando:

```
Router# clear ip nat translation *
```

A continuación cambien el timeout de las conversiones dinámicas con el comando:

```
Router(config)# ip nat translation timeout segundos
```

Donde `segundos` es el número máximo de segundos de inactividad antes de borrar una entrada de conversión

- Configuren un número pequeño de segundos
- Repitan el proceso de ir cambiando la dirección IP del PC B y haciendo ping para agotar de nuevo el pool de direcciones. Cuando falle la conversión por agotamiento dejen el ping un rato hasta que expire el timeout de alguna de las conversiones que ya no se están empleando, momento en el cual empezará a funcionar. Vean cómo cambia la tabla de conversiones.

También pueden ver estadísticas con el comando `show ip nat statistics`.

Checkpoint 12.2: Muestren al profesor de prácticas que les funciona.

Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

## 7- Sobrecarga de la dirección exterior del router

En este apartado vamos a configurar que el router convierta todas las direcciones internas en *su* dirección externa.

- Modifiquen la topología de la figura 1 añadiendo un PC3 a la Red B (ver figura 2)

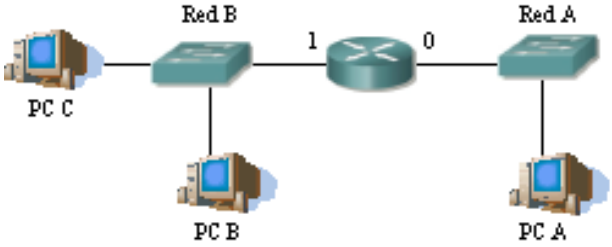


Figura 2.- Dos redes y 3 PCs

De lo que han aprendido para la configuración con un pool necesitarán crear una lista de acceso como la que crearon en ese ejercicio. Lo que no necesitaremos es el pool, dado que la IP del router es todo el pool disponible.

- Activamos NAT con el siguiente comando:

```
Router(config)# ip nat inside source list 1 interface elifexterno overload
```

Donde `elifexterno` debe ser el nombre del interfaz del router conectado al exterior.

- Una vez hecho esto (y especificado el interfaz interior y el exterior) prueben a conectarse por ssh al PC A desde el PC B y desde el PC C simultáneamente
- Vean las entradas que aparecen en la tabla de conversiones y vean los paquetes en las dos redes con `tcpdump`.

## 8- Conexión a la red del laboratorio empleando NAT

- A continuación preparen la disposición física de la figura 3

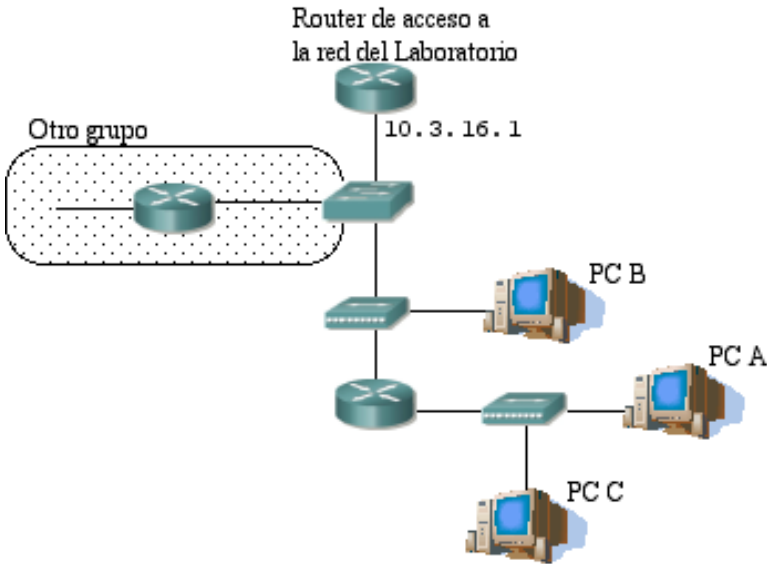


Figura 3.- Router a la red del laboratorio

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

Empleen el espacio de direcciones `192.168.0.0/24` en la red interna.

- Activen que el router haga NAT empleando como dirección externa solo la de su interfaz que debe ser la `10.3.17.armario /20`
- Que PC B no tenga dirección IP
- Realicen conexiones a máquinas del laboratorio desde PC A y PC C
- Vean los paquetes con tcpdump en la red interior y la red exterior. ¿Hace falta modificar la tabla de rutas del router de acceso?

Checkpoint 12.3: Expliquen al profesor de prácticas cómo funciona esta conversión.

## *9- Redirección de puertos (opcional)*

Utilicen el escenario del apartado anterior para configurar en su router de acceso la siguiente redirección de puertos.

| Puertos públicos | Puertos privados | IP privada | PC |
|---|---|---|---|
| 5001 | 5010 | <ipPCA> | A |
| 5002 | 5020 | <ipPCC> | C |

- Para comprobar su configuración, ponga dos servidores, uno en PC A y otro en PC C, mediante el programa netcat(comando nc) en los puertos indicados en la tabla anterior y conéctese a ellos desde cualquier equipo con acceso a la red del laboratorio, mediante el mismo comando nc o mediante telnet a los puertos públicos respectivos.

Checkpoint opcional: Muestre al profesor de prácticas que le funciona la redirección de puertos.