Práctica 4: Conversión de direcciones IP: NAT y PAT. Conexión a Internet.

1.- Objetivos

El objetivo de esta práctica es familiarizarse con:

- Escalabilidad y conservación de direcciones IPv4.
- Direccionamiento público y privado.
- Conversión de direcciones de red IP: NAT estática y NAT dinámica.
- Sobrecarga de NAT con la conversión de direcciones de puerto: PAT.
- Conexión a Internet.
- DNS.

Para ello, se construirá en el simulador una red sencilla mediante switches y routers que conecten diferentes equipos. En esta práctica se busca configurar apropiadamente todos los equipos de la red para que puedan comunicarse correctamente entre sí. Esto se realizará mediante la interfaz de comandos de la IOS de Cisco.

2.- Conocimientos previos

2.1.- Perspectivas sobre la escalabilidad de direcciones en IPv4

El diseño original de Internet requería que todas las organizaciones solicitasen y recibiesen uno o más números de red IP con clase registrados. Quienes administraban el programa se aseguraban de que no se reutilizase ninguna de las direcciones IP.

A principios de los 90, Internet crecía tan deprisa que todos los números de red IP se habrían reservado a mediados de la década. Se temía que las redes disponibles quedasen completamente reservadas y que algunas organizaciones no pudieran conectarse a Internet.

La solución principal a largo plazo para este problema consistía en incrementar el tamaño de la dirección IP, de ahí el advenimiento de IPv6.

Se sugirieron muchas soluciones a corto plazo para el problema del direccionamiento, pero hay dos estándares que cooperan estrechamente para resolver el problema: Conversión de direcciones de red (NAT) y el direccionamiento privado. Estos mecanismos, en su conjunto, permiten a las organizaciones utilizar internamente números IP no registrados, y comunicarse perfectamente con Internet.

2.2.- Direccionamiento privado

La RFC 1918 define un conjunto de redes que nunca serán asignadas a ninguna organización como número de red registrado. En lugar de utilizar los números de red registrados de alguna otra empresa, se pueden utilizar números de un rango que no va a ser utilizado por nadie más dentro de la Internet pública.

En otras palabras, cualquier organización puede emplear estos números de red. Sin embargo, no se permite que ninguna organización publique estas redes empleando un protocolo de enrutamiento en Internet.

Table 18-2 *RFC 1918 Private Address Space*

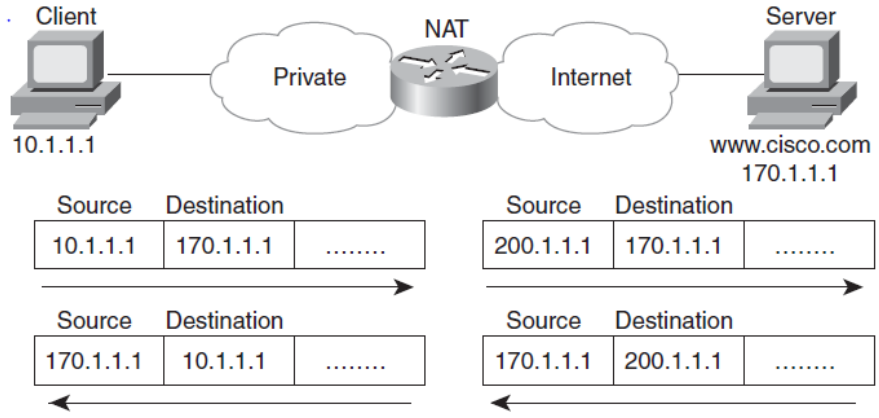
Range of IP Addresses	Class of Networks	Number of Networks
10.0.0.0 to 10.255.255.255	A	1
172.16.0.0 to 172.31.255.255	B	16
192.168.0.0 to 192.168.255.255	C	256

2.3.- Conceptos de Conversión de Direcciones de Red (NAT, *Network Address Translation)*

NAT (RFC 3022) permite a un host que no tiene una dirección IP globalmente exclusiva, registrada y válida, comunicarse con otros hosts a través de Internet. Este host podría usar direcciones privadas o direcciones asignadas a otra organización. En ambos casos, NAT permite seguir utilizando estas direcciones que no están preparadas para Internet y sigue permitiendo las comunicaciones con otros hosts a través de Internet.

NAT consigue este objetivo empleando una dirección IP válida registrada para representar la dirección privada frente al resto de Internet. La funcionalidad de NAT cambia las direcciones IP privadas por direcciones IP registradas públicamente dentro de cada paquete, según se muestra en la siguiente figura. El router que lleva a cabo NAT también modifica la dirección de destino de todos los paquetes que se reenvían hacia la red privada.

Figure 18-2 *NAT IP Address Swapping: Private Addressing*

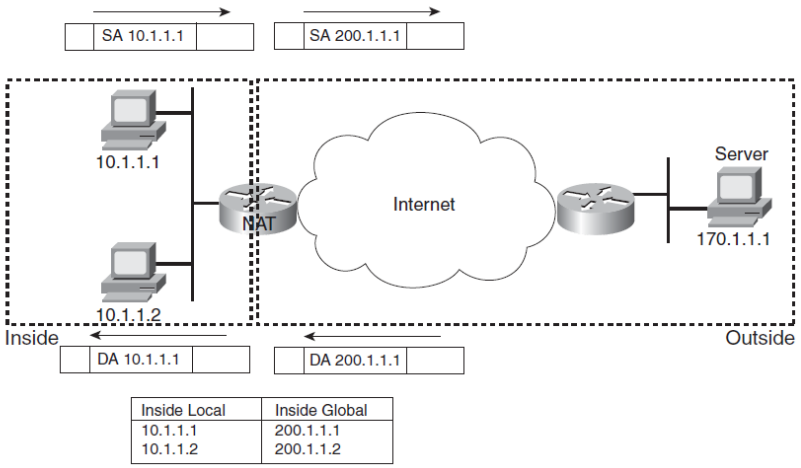


2.4.- NAT estática

La NAT estática funciona exactamente igual que el ejemplo anterior, pero con direcciones IP asignadas entre sí estáticamente.

En el ejemplo siguiente el ISP ha asignado la red registrada 200.1.1.0. Por tanto, el router NAT tiene que hacer que las direcciones IP privadas parezcan estar en la red 200.1.1.0. Para lograr esto, el router NAT cambia las direcciones IP origen que hay en los paquetes que van de izquierda a derecha en la figura.

Figure 18-4 *Static NAT Terminology*



En este ejemplo, el router NAT modifica la dirección de origen (*Source Addess*, SA) de 10.1.1.1 a 200.1.1.1. Al emplear NAT estática, el router se limita a configurar una asignación de "uno a uno" entre la dirección privada y la pública. Para admitir un segundo host IP en la red privada se necesita una segunda asignación de "uno a uno" estática, empleando una segunda dirección IP del rango público.

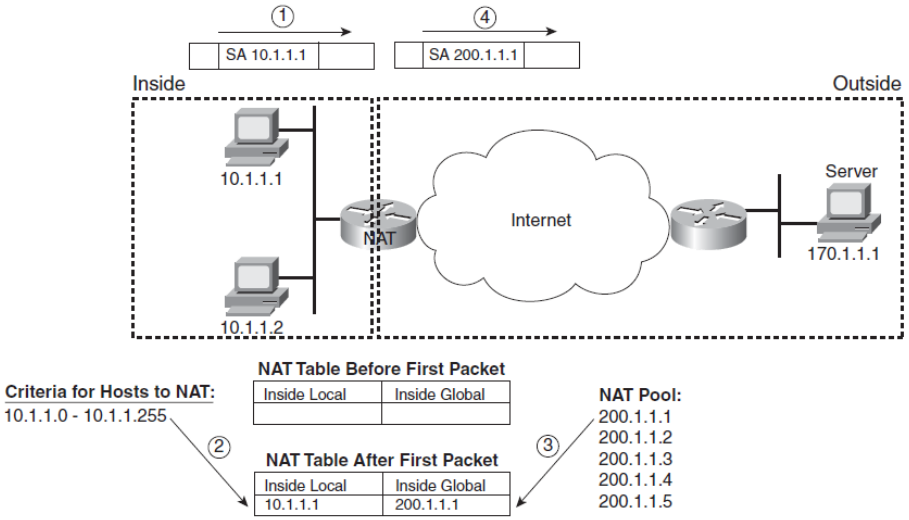
Cisco utiliza el término **Inside Local** para las direcciones IP privadas que se utilizan en la red interna y el término **Inside Global** para las direcciones IP públicas que se utilizan para representar al host de la red interna en el resto de Internet.

2.5.- NAT dinámica

Al igual que la NAT estática, el router NAT crea una asignación "de uno a uno", sin embargo el mapeo de una dirección local interna a una dirección global interna se produce dinámicamente.

La NAT dinámica establece un almacén (*pool*) de direcciones globales internas posibles, y define los criterios correspondientes para determinar qué direcciones IP locales internas deberían convertirse mediante NAT.

Figure 18-5 *Dynamic NAT*



La siguiente figura muestra cómo se ha configurado NAT dinámica en el ejemplo de la figura anterior. Cada paso está explicado posteriormente, en el apartado 2.7.

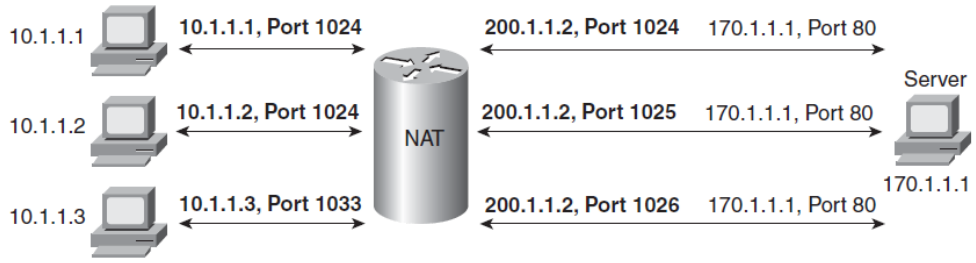
Example 18-2 *Dynamic NAT Configuration*

```
NAT# show running-config
!
! Lines omitted for brevity
!
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip nat inside
!
interface Serial0/0
 ip address 200.1.1.251 255.255.255.0
 ip nat outside
!
ip nat pool fred 200.1.1.1 200.1.1.2 netmask 255.255.255.252
ip nat inside source list 1 pool fred
!
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.1
! The next command lists one empty line because no entries have been dynamically
! created yet.
NAT# show ip nat translations
```

2.6.- Sobrecarga de NAT con traducción de direcciones de puerto (Port Address Translation, PAT)

La sobrecarga de NAT (NAT/PAT) permite dar soporte a muchos clientes con sola una o unas pocas direcciones IP públicas. NAT/PAT se aprovecha de que a un servidor no le importa si tiene una conexión a tres hosts distintos o tres conexiones a diferentes puertos del mismo host con una sola dirección IP. Por tanto, para admitir muchas direcciones IP locales internas, PAT convierte tanto las direcciones como posiblemente también los números de puerto. La siguiente figura ilustra la lógica.

Figure 18-7 *NAT Overload (PAT)*



Dynamic NAT Table, With Overloading

Inside Local	Inside Global
10.1.1.1:1024	200.1.1.2:1024
10.1.1.2:1024	200.1.1.2:1025
10.1.1.3:1033	200.1.1.2:1026

El router NAT mantiene una entrada en la tabla NAT para cada combinación exclusiva de dirección IP local interna y número de puerto, efectuando una conversión a la dirección global interna y un número exclusivo de puerto asociados a la dirección global interna. Como el

número de puerto tiene 16 bits, PAT puede utilizar más de 65.000 números de puerto, lo que permite crecer con sólo una dirección IP pública.

PAT es con mucho la opción más popular y es la que analizaremos en la práctica.

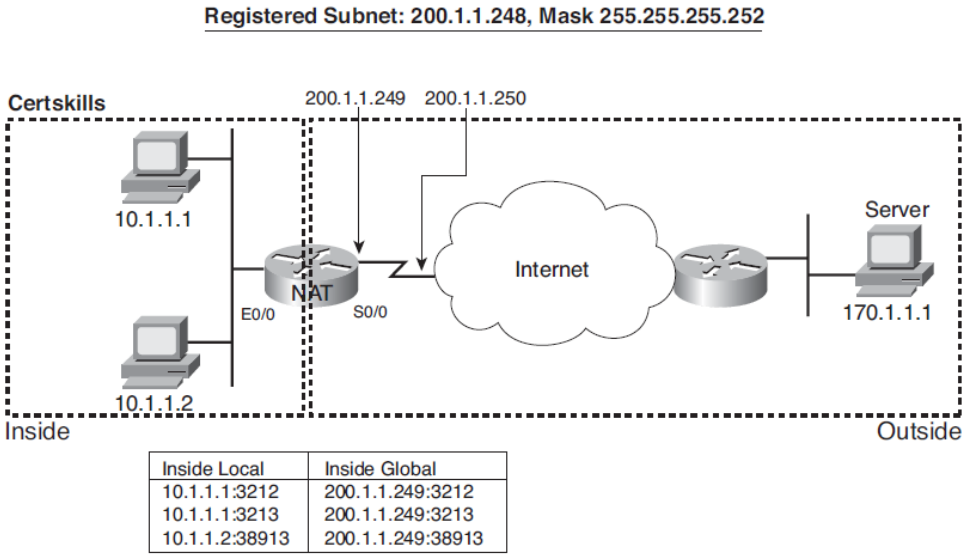
2.7.- Configuración de sobrecarga NAT (PAT) en Cisco IOS

La siguiente lista muestra la configuración que hay que efectuar cuando se utiliza un pool de direcciones IP como única dirección IP global interna:

1. Tanto para NAT estática como dinámica, se configuran las interfaces internas con el subcomando de interface: **ip nat inside**.
2. Tanto para NAT estática como dinámica, se configuran las interfaces externas con el subcomando de interface: **ip nat outside**.
3. Para NAT dinámica, es necesario configurar al menos una ACL (Access Control List) que especifique (admita) aquellos paquetes que provengan de interfaces internas, como en el ejemplo del apartado 2.5: **access-list** *número-de-acl* **permit** *ip-interna*
4. Se configura el almacén de direcciones IP registradas públicas (un rango de IPs) empleando el comando de configuración global:
   ip nat pool *nombre-almacén primera-dirección última-dirección* **netmask** *máscara-red*
   La *máscara-red* es la de las direcciones del almacén y se incluye solo para verificación.
5. Se activa NAT mediante el siguiente comando de configuración global. Si se incluye la palabra opcional "overload", se activa también PAT:
   ip nat inside source list *número-de-acl* **pool** *nombre-almacén* [**overload**]

Una vez configurado, el comando **show ip nat translations** muestra la tabla NAT. Veamos un ejemplo completo, que emplea la misma ACL 1 definida previamente en el ejemplo del apartado 2.5.

Figure 18-10 *NAT Overload and PAT*



Inside Local	Inside Global
10.1.1.1:3212	200.1.1.249:3212
10.1.1.1:3213	200.1.1.249:3213
10.1.1.2:38913	200.1.1.249:38913

Example 18-4 *NAT Overload Configuration*

```
NAT# show running-config
!
! Lines Omitted for Brevity
!
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip nat inside
!
interface Serial0/0
 ip address 200.1.1.249 255.255.255.252
 ip nat outside
!
ip nat inside source list 1 interface Serial0/0 overload
!
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.1
!

NAT# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.1.1.249:3212   10.1.1.1:3212      170.1.1.1:23       170.1.1.1:23
tcp 200.1.1.249:3213   10.1.1.1:3213      170.1.1.1:23       170.1.1.1:23
tcp 200.1.1.249:38913  10.1.1.2:38913     170.1.1.1:23       170.1.1.1:23
```

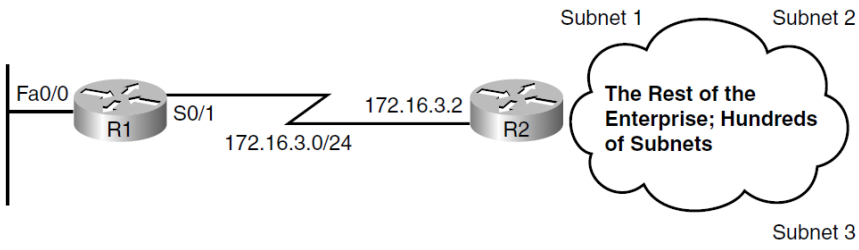
El simulador no permite el overload de una interfaz (como en este ejemplo), pero sí de un pool como se ha indicado antes. Como hemos visto antes, se configura igual que NAT dinámica añadiendo el comando **overload.**

2.8.- Rutas por defecto

En ocasiones resulta interesante asignar una ruta por defecto (*default route*), que se empleará cuando la red de destino no se encuentre en la tabla de encaminamiento del router. Estas rutas por defecto se emplean típicamente para enviar el tráfico dirigido al exterior hacia Internet, o bien para encaminar tráfico hacia el "*core*" de la red.

Para establecer una ruta por defecto en un router basta con añadir una ruta estática a la red de destino 0.0.0.0/0. Cualquier paquete coincide con esta regla, ya que no fuerza ningún bit; sin embargo, las normas de IP dicen que un router debe encaminar el tráfico de acuerdo a la regla más específica (es decir, con la máscara más larga) que tenga en la tabla. Por este motivo, la ruta por defecto solo se empleará cuando no haya otra ruta.

La siguiente figura muestra un ejemplo. Al router R1 no le interesa conocer todas las rutas que hay en la empresa, ya que solo tiene una única vía de salida, sea cual sea el destino. Se puede activar una ruta por defecto y se puede desactivar el protocolo de encaminamiento.



```
R1(config)#ip route  0.0.0.0  0.0.0.0  172.16.3.2
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route


Gateway of last resort is 172.16.3.2 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.3.0 is directly connected, Serial0/1
S*      0.0.0.0/0 [1/0] via 172.16.3.2
```

Para configurar una ruta predeterminada se utiliza el comando:

ip route 0.0.0.0 0.0.0.0 *dirección_siguiente_salto*

o

ip route 0.0.0.0 0.0.0.0 *interface saliente* [solo en enlaces serie punto-a-punto]

3.- Desarrollo de la práctica

En la práctica se busca que nos familiaricemos con la conversión de direcciones IP mediante NAT/PAT. Para ello, vamos a crear y probar una configuración de red para una empresa. Gracias a esta configuración toda la empresa podrá navegar por Internet compartiendo una única dirección IP pública.

3.1 Configuración de un router con NAT/PAT. Conexión a un ISP (Internet Service Provider).

a) Disponer un switch y conectarle tres PCs. Configurar los PCs con direcciones IP fijas pertenecientes a la red 10.10.10.0/24. (Red A).
b) Desplegar un router A con al menos un puerto Ethernet y un puerto serie, y conectarlo al switch A. Configurar la interfaz Ethernet del router con la primera dirección de la red A. Configurar apropiadamente el Gateway por defecto en los PCs.
c) Disponer una nube ISP ("to Internet") y conectarla al router A con una conexión WAN serial. Leer atentamente las instrucciones de la nube ISP haciendo doble click sobre el icono de la nube (pestañas "*What the…"* e *"ISP Configuration"*).
d) Configurar una ruta por defecto en el router A para todas las redes desconocidas.
e) Disponer un router B. Conectar la nube ISP a este router B. Conectar un PC a este router. Configurar el PC y el router con una dirección IP pública de una subnet /27 de la clase asignada por el ISP al conectarlo. Esta red B hará las veces de un servicio de Internet cualquiera. ¿Hará falta una ruta por defecto?
f) Disponer un router C. Conectar la nube ISP a este router C. Conectar un PC a éste router. Configurar el PC y el router con una dirección IP pública de una subnet /27 de la clase asignada por el ISP al conectarlo. Esta red C hará las veces de otro servicio de Internet cualquiera. ¿Hará falta una ruta por defecto?
g) Comprobar que hay conectividad entre las redes B y C.
h) ¿Se puede acceder desde la Red A, a las redes B y C? ¿Por qué?
i) Configurar NAT/ PAT en el router A como se ha explicado en el apartado *Conocimientos previos*. Para el pool utilizar una subnet /27 de la clase asignada por el ISP al conectarla al router A.
j) Mostrar las conversiones NAT.
k) ¿Se puede acceder ahora desde la Red A, a las redes B y C? ¿Por qué?

3.2 Configuración de un servidor DNS y un servidor Web. Navegación por Internet.

a) Activar en el PC de la red B el servidor Web.
b) Activar en el PC de la red C el servidor DNS. Configurarlo con la entrada www.practica.es apuntando al servidor B.
c) Configurar apropiadamente los PCs de la red A.
d) Comprobar que desde la red A se navega por www.practica.es y también se hace ping a www.practica.es.

Bibliografía

CCENT/CCNA ICND1 Guía Oficial para el examen de Certificación, Wendell Odom, Cisco Press.

CCNA ICND2 Guía Oficial para el examen de Certificación, Wendell Odom, Cisco Press.