Laboratorio 9: NAT/NAPT

Objetivos:

1. Profundizar en el concepto y fundamentos de la tecnología NAT[1].
2. Conocer la configuración básica de NAT en el sistema IOS.

Topología de trabajo

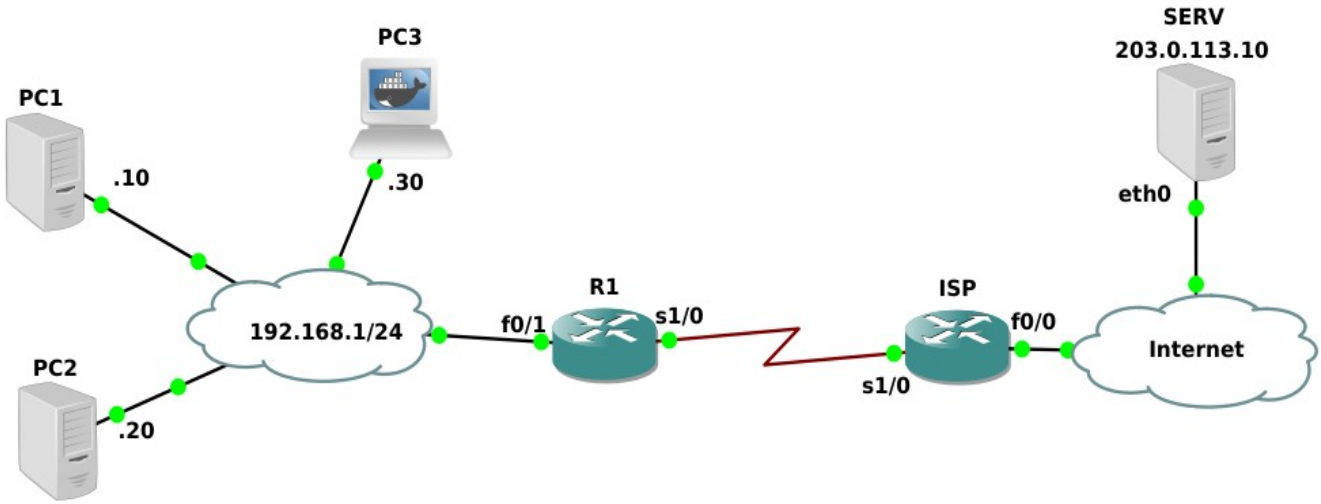

Figura 1 : Red utilizada

Nuestro ISP nos ha cedido el rango de direcciones públicas[2] `198.51.100.160/30`.

Tareas

Preparativos:

1. Para empezar, desde *e-gela*, descarga el proyecto con la configuración de la red, y descomprímela en el directorio `GNS3/projects`.
2. Lanza GNS3, abre el proyecto descargado. Verifica el nombre de las interfaces, pon en marcha todas las máquinas (excepto `PC3`) y abre todas las consolas.
3. Haz `ping` de `SERV` a `PC1` o `PC2`. ¿Por qué no recibes una respuesta?

[1] https://ccnadesdecero.es/nat-network-address-translation/
https://ccnadesdecero.es/configuracion-nat-estatica-dinamica-pat/
https://www.practicalnetworking.net/stand-alone/cisco-nat-configurations-ios-router/
https://www.rfc-es.org/rfc/rfc3022-es.txt

[2] El rango de direcciones no es realmente público, es un rango reservado para documentación (RFC 5737)

Configurar NAT estático:

4. Supongamos que necesitas instalar dos servidores en `PC1` y en `PC2`, y quieres que sean visibles desde Internet. Por otro lado, los usuarios internos trabajan con direcciones IP privadas. ¿Cómo lo conseguirías?

5. Establece la siguiente configuración NAT:

Interfaz interna	**Dirección pública**
`PC1-eth0`	`198.51.100.161`
`PC2-eth0`	`198.51.100.162`

   Pasos:

   a) Define la interfaz interna y la externa en el encaminador R1:
   R1(config-if)# **ip nat inside**
   R1(config-if)# **ip nat outside**
   b) Define la traducción estática especificada:
   R1(config)# **ip nat inside source static** *dir_local dir_global*

6. Verifica la configuración realizada en `R1`:
   - NAT está habilitado en las interfaces: **sh ip nat stat**
   - Consulta la tabla NAT: **sh ip nat trans [verbose]**
   - Para analizar cómo `R1` traduce cada paquete, activa/desactiva: **(no) debug ip nat**

7. Haz `ping` de `PC1` a `SERV`, y analiza la tabla NAT en `R1`. ¿Cuáles son las diferencias que observas, con respecto a la tabla NAT anterior?

8. Establece una conexión remota desde `PC1` a `ISP-s1/0` (**telnet** *dir_IP*) y analiza la tabla NAT en `R1`. ¿Cuáles son las diferencias que observas, con respecto a la tabla NAT anterior?

9. Comprueba ahora que `PC1` y `PC2` son visibles para cualquier máquina que está en Internet. ¿Cómo lo harás? ¿Qué dirección IP hay que usar para acceder a `PC1`?

10. Revisa las estadísticas del servidor NAT (**sh ip nat statistics**).

Configurar NAT dinámico (#internas = #externas):
(Dynamic one-to-one NAT)

11. Detén el acceso remoto del apartado 8 (`ISP> quit`). Deshaz la anterior configuración estática de NAT.

12. Configura un NAT dinámico, que asigne las direcciones públicas `198.51.100.161/30` y `198.51.100.162/30` únicamente a cualquiera de las dos máquinas `PC1` o `PC2` de la red interna.

    Pasos:

    a) Define la interfaz interna y la externa en el encaminador R1 (ya lo has realizado)
    b) Define la lista de direcciones locales a las que puede aplicarse NAT:
    R1(config)# **access-list** *num_identif_lista* **permit** *dir_IP wildcard*
    c) Define el grupo de direcciones públicas (*pool*) que se utilizarán:

R1(config)# **ip nat pool** *NOMBRE dirIP_inicial dirIP_final* **prefix-length** *longitud*

d) Establece la correspondencia entre la lista de direcciones locales con el grupo de direcciones públicas:

R1(config)# **ip nat inside source list** *num_identif_lista* **pool** *NOMBRE*

13. Haz un `ping` de `PC2` a `SERV`, y luego otro de `PC1` a `SERV`. Ahora echa un vistazo a la tabla NAT en `R1` y verifica si se mantiene la asignación de la dirección que hizo antes.

Configurar NAPT dinámico (#internas > #externas > 1):
(PAT / NAT con sobrecarga)

14. Pon en marcha la máquina `PC3`. Configura un NAT dinámico, que asigne las direcciones públicas `198.51.100.161/30` y `198.51.100.162/30` a cualquier máquina de la red interna. Antes, hay que deshacer la asignación dinámica de la configuración NAT anterior.

    Pasos:

    a) y c) Ya están hechos.
    b) Definir la lista de direcciones locales.
    d) Similar pero se debe agregar la opción de sobrecarga (*overload*)

    R1(config)# **ip nat inside source list** *identif_lista* **pool** *NOMBRE* **overload**

15. Haz `ping` desde cada uno de los tres `PC`'s en la red interna a `SERV`, y luego revisa la tabla NAT en `R1`.

IP masquerading (Enmascaramiento IP):
(NAPT dinámico, donde #internas > #externas = 1)
(PAT con dirección única / NAT con sobrecarga con dirección única)

16. Supongamos que ya no disponemos del bloque de direcciones públicas `198.51.100.160/30`. Deshaz la configuración NAT que permitía usar estas direcciones públicas.
17. Supongamos que usamos el subconjunto `192.168.1.0/25` en la red interna para las máquinas que tienen autorizado el acceso a Internet y la otra mitad, `192.168.1.128/25`, para aquellas que no lo tienen.
18. Configura NAT para que todas las máquinas que tienen autorizado el acceso a Internet utilicen la dirección pública de la interfaz `R1-s1/0`.

    Pasos:

    a) Define la interfaz interna y la externa en el encaminador R1 (ya lo has realizado)
    b) Define la lista de direcciones locales a las que puede aplicarse NAT
    c) Vincula la lista definida a la interfaz que tiene la dirección global

    R1(config)# **ip nat inside source list** *num_identif_lista* **interface** *interfaz* **overload**

19. Verifica que la tabla NAT en `R1` está vacía. Después, haz `ping` desde cada `PC` a `SERV`. Examina la tabla NAT en `R1`. Si quieres realizar un `ping` desde `SERV` a cualquier `PC`, ¿qué dirección le darás al programa `ping`?

20. Añade una nueva máquina `PC4`. Realiza su configuración `IP`, asignándole la dirección IP `192.168.1.200`. Haz un `ping` desde la nueva máquina a `SERV`. ¿Funciona? ¿Por qué?

Análisis del funcionamiento NAT

21. Con los datos recogidos en la tabla NAT del ejercicio anterior, completa la siguiente tabla correspondiente al `ping` realizado desde `PC1`:

	En la red 192.168.1/24		***En Internet***	
	Origen (IP:puerto)	*Destino (IP:puerto)*	*Origen (IP:puerto)*	*Destino (IP:puerto)*
ICMP echo request				
ICMP echo reply				

22. Para verificar si se ha completado correctamente o no la tabla, realiza capturas dentro y fuera de la red con *Wireshark* en el enlace de `PC1` a `SERV`; configúralo para capturar tráfico ICMP y repite el `ping`. Examina el tráfico capturado a ver si es consistente con el contenido de la tabla (ten en cuenta los cambios en puertos; tal vez tengas que rehacer tu tabla).

23. Establece una conexión remota desde `PC1` a `ISP-s1/0` y analiza la tabla NAT en `R1`. Con los datos mostrados en la tabla NAT, completa la siguiente tabla:

	En la red 192.168.1/24		***En red de acceso***	
	Origen (IP:puerto)	*Destino (IP:puerto)*	*Origen (IP:puerto)*	*Destino (IP:puerto)*
Telnet - - >				
< - - Telnet				