Configuración en Cisco Packet Tracer: NAT y PAT en un router Cisco

1. Introducción

En este documento se presenta la configuración de **NAT (Network Address Translation)** en un router Cisco para permitir la comunicación entre una red privada y una red pública (Internet). Se abordarán tres tipos de NAT:

NAT Estático: Asigna manualmente una IP pública a un dispositivo específico.
NAT Dinámico: Permite que múltiples dispositivos usen una o varias IPs públicas de manera dinámica.
PAT (Port Address Translation / Sobrecarga): Todos los dispositivos comparten una única IP pública, diferenciándose por puertos.

2. Topología de Red

La infraestructura utilizada en este laboratorio consta de los siguientes dispositivos:

Dispositivo	IP Asignada	Máscara	Gateway
PC0	10.1.0.2	255.255.255.0	10.1.0.1
PC1	10.1.0.3	255.255.255.0	10.1.0.1
PC2	10.1.0.4	255.255.255.0	10.1.0.1
Switch			
Router (LAN)	10.1.0.1	255.255.255.0	-
Router (WAN)	172.22.34.123	255.255.255.0	172.22.34.1
Servidor-Server0 (Internet)	172.22.34.1	255.255.255.0	172.22.34.123

3. Configuración del Router

Paso 1: Asignación de IPs a interfaces

- Accedemos al router y entramos en modo de configuración global:

```
enable
configure terminal
```

- Configuramos la interfaz interna (hacia los PCs):

```
interface GigabitEthernet0/0
ip address 10.1.0.1 255.255.255.0
no shutdown
exit
```

- Configuramos la interfaz externa (hacia Internet):

```
interface GigabitEthernet0/1
ip address 172.22.34.123 255.255.255.0
no shutdown
exit
```

- Definimos qué interfaz es interna y cuál es externa para NAT:

```
interface GigabitEthernet0/0
ip nat inside
exit


interface GigabitEthernet0/1
ip nat outside
exit
```

Explicación:

- gigabitethernet0/0 es la interfaz conectada a la red interna.
- gigabitethernet0/1 es la interfaz conectada a Internet.

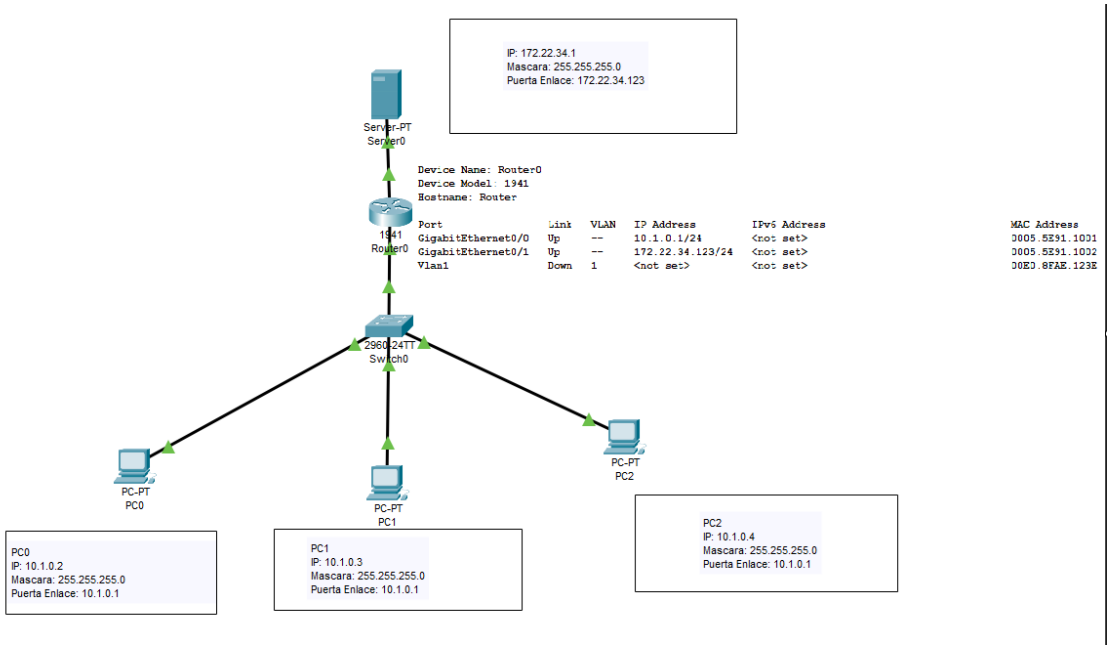

Ilustración 1: Topología de Red

4. Configuración de NAT Estático

El **NAT Estático** se usa para asignar una IP privada específica a una IP pública fija.

Objetivo

- El **PC0 (10.1.0.2)** tendrá una IP pública estática **172.22.34.124**
- Esto permite que **PC0** sea accesible desde Internet con una IP fija.

Configuración

- **Comandos** en el Router

  enable
  configure terminal

- **Asignamos NAT Estático** para PC1:
  ip nat inside source static 10.1.0.2 172.22.34.124

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static 10.1.0.2 172.22.34.124
Router(config)#
```

Ilustración 2: ip nat inside source static 10.1.0.2 172.22.34.124

- **Definimos** las interfaces:
  interface GigabitEthernet0/0
  ip address 10.1.0.1 255.255.255.0
  ip nat inside
  no shutdown
  exit

```
interface GigabitEthernet0/1
ip address 172.22.34.123 255.255.255.0
ip nat outside
no shutdown
exit
```

Comprobaciones:

- Desde el Router:
  Vemos la tabla de NAT:
  show ip nat translations

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  172.22.34.124     10.1.0.2           ---                ---

Router#
```

Ilustración 3: show ip nat translations

- Desde el Servidor (Server0)
  Hacemos ping a 172.22.34.124:
  ping 172.22.34.124

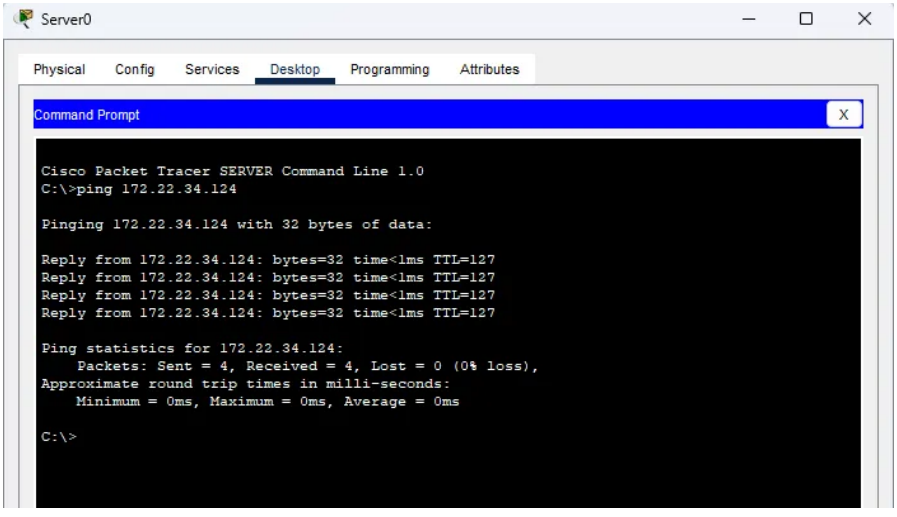

Ilustración 4: ping 172.22.34.124

Como vemos en la Ilustración 4 responde al ping, significa que la traducción funciona correctamente.

5. Configuración de NAT Dinámico

El NAT Dinámico asigna una IP pública de un pool a varias IPs privadas. En este caso, PC2 (10.1.0.3) y PC3 (10.1.0.4) usarán NAT Dinámico con una única IP pública.

Objetivo

- **PC1 (10.1.0.3) y PC2 (10.1.0.4)** usarán una IP pública dinámica.
- Como solo tenemos **una IP pública (172.22.34.123)**, se les asignará de manera dinámica.

Configuración

- Comandos en el Router

1. **Creamos una ACL(Lista de Control de Acceso)**para definir qué IPs privadas pueden salir a Internet:

access-list 1 permit 10.1.0.3
access-list 1 permit 10.1.0.4

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 1 permit 10.1.0.3
Router(config)#access-list 1 permit 10.1.0.4
```

Ilustración 5: access-list 1 permit 10.1.0.3

2. **Definimos un pool** de IPs públicas:

ip nat pool MiPool 172.22.34.123 172.22.34.123 netmask 255.255.255.0

```
Router(config)#ip nat pool MiPool 172.22.34.123 172.22.34.123 netmask 255.255.255.0
Router(config)#
```

Ilustración 6: ip nat pool MiPool 172.22.34.123 172.22.34.123 netmask 255.255.255.0

3. **Asociamos la ACL(Lista de Control de Acceso)** con el pool de NAT:

ip nat inside source list 1 pool MiPool

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

Ilustración 7: ip nat inside source list 1 pool MiPool

Comprobaciones

- Desde PC 1 **(10.1.0.3)**::
  ping 172.22.34.1

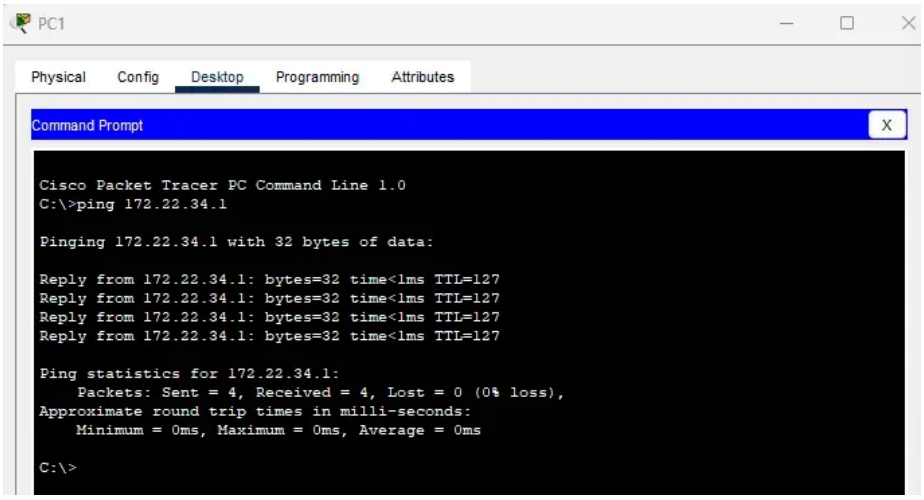

Ilustración 8: ping 172.22.34.1

- Desde del PC 2 **(10.1.0.4)**:
  ping 172.22.34.1

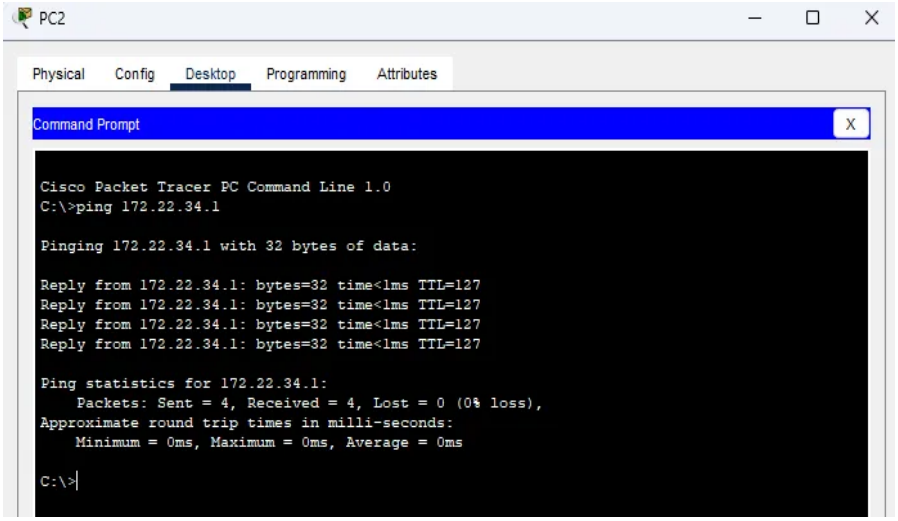

Ilustración 9: ping 172.22.34.1

Tanto en la Ilustración 8 como en la Ilustración 9 vemos que responde al ping, significa que NAT Dinámico esta funcionando correctamente

- Desde el Router:
  show ip nat translations

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 172.22.34.123:1   10.1.0.3:1         172.22.34.1:1      172.22.34.1:1
icmp 172.22.34.123:2   10.1.0.3:2         172.22.34.1:2      172.22.34.1:2
icmp 172.22.34.123:3   10.1.0.3:3         172.22.34.1:3      172.22.34.1:3
---  172.22.34.124     10.1.0.2           ---                ---
```

Ilustración 10: show ip nat translations

Para verificar que el NAT Dinámico está funcionando, ejecutamos **show ip nat translations**. La tabla obtenida en la ilustracion 10 nos muestra:

- Las IPs privadas **(10.1.0.3, 10.1.0.4)** se traducen dinámicamente a la IP pública (172.22.34.123).
- Los valores en la columna icmp indican que los dispositivos están enviando paquetes de ping a un destino externo (172.22.34.1).
- Esto confirma que **NAT Dinámico** está asignando correctamente la IP pública de manera dinámica a los dispositivos internos.

6. Configuración de PAT (NAT Sobrecargado)

El **PAT (Port Address Translation)** permite que **múltiples dispositivos compartan una sola IP pública diferenciándolos por puerto**.

Objetivo

- Todos los PCs (10.1.0.2, 10.1.0.3 y 10.1.0.4) compartirán la misma IP pública **172.22.34.123** usando PAT.

Configuración

1. **Creamos una ACL(Lista de Control de Acceso)** para definir qué IPs privadas pueden salir a Internet:

access-list 1 permit 10.1.0.0 0.0.0.255

```
Router(config)#access-list 1 permit 10.1.0.0 0.0.0.255
Router(config)#
```

Ilustración 11: access-list 1 permit 10.1.0.0 0.0.0.255

2. **Configuramos PAT** para que todas las IPs usen la interfaz pública:

ip nat inside source list 1 interface GigabitEthernet0/1 overload

```
Router(config)#ip nat inside source list 1 interface GigabitEthernet0/1 overload
Router(config)#
```

Ilustración 12: ip nat inside source list 1 interface GigabitEthernet0/1 overload

Comprobaciones

- Desde PC0:
  Abrimos la terminal y ejecutamos:
  telnet 172.22.34.1

- Desde PC1:
  Abrimos la terminal y ejecutamos:
  telnet 172.22.34.1

- Desde PC2:
  telnet 172.22.34.1

- Ahora, en el router, ejecutamos:
  show ip nat translations

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 172.22.34.123:1027 10.1.0.3:1027      172.22.34.1:23     172.22.34.1:23
tcp 172.22.34.123:1028 10.1.0.2:1028      172.22.34.1:23     172.22.34.1:23
tcp 172.22.34.123:1029 10.1.0.4:1029      172.22.34.1:23     172.22.34.1:23
```

Ilustración 13: show ip nat translations

Al ejecutar este comando, podemos ver la tabla de NAT, como se muestra en la ilustración 13. Esta tabla contiene cuatro columnas principales:

- **Inside Local:** Muestra la IP privada del dispositivo en la LAN antes de la traducción.
- **Inside Global:** Indica la IP pública asignada al dispositivo mediante NAT.
- **Outside Local:** Representa la IP del destino desde la perspectiva de la LAN.
- **Outside Global:** Es la IP real del destino en Internet.

Explicación de los valores en la tabla:

- 10.1.0.2:1025 corresponde a la conexión del **PC0**, donde 1027 es el puerto asignado por PAT.
- 10.1.0.3:1026 pertenece al **PC1**, utilizando un puerto diferente (1028).
- 10.1.0.4:1027 es la conexión del **PC2**, con otro puerto (1029).
- Todos los dispositivos están traducidos a la misma IP pública 172.22.34.123, pero con puertos distintos para evitar conflictos.

Esto confirma que **PAT está funcionando correctamente**, permitiendo que múltiples dispositivos compartan la misma IP pública sin interferencias.

En la ilustración 14, se observa que los valores en la tabla de NAT no representan puertos reales, sino identificadores de solicitud ICMP, ya que la prueba se realizó con ping en lugar de Telnet.

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 172.22.34.123:1024 10.1.0.3:13       172.22.34.1:13     172.22.34.1:1024
icmp 172.22.34.123:1025 10.1.0.3:14       172.22.34.1:14     172.22.34.1:1025
icmp 172.22.34.123:1026 10.1.0.3:15       172.22.34.1:15     172.22.34.1:1026
icmp 172.22.34.123:1027 10.1.0.3:16       172.22.34.1:16     172.22.34.1:1027
icmp 172.22.34.123:10   10.1.0.4:10       172.22.34.1:10     172.22.34.1:10
icmp 172.22.34.123:13   10.1.0.2:13       172.22.34.1:13     172.22.34.1:13
icmp 172.22.34.123:14   10.1.0.2:14       172.22.34.1:14     172.22.34.1:14
icmp 172.22.34.123:15   10.1.0.2:15       172.22.34.1:15     172.22.34.1:15
icmp 172.22.34.123:16   10.1.0.2:16       172.22.34.1:16     172.22.34.1:16
icmp 172.22.34.123:9    10.1.0.4:9        172.22.34.1:9      172.22.34.1:9
```

Ilustración 14: ping 172.22.34.1

¿Por qué hago la comprobación con Telnet en NAT?

Yo prefiero hacer la comprobación con **Telnet** en lugar de solo usar **ping**, aunque ambos aparecen en la tabla de NAT.

El **ping (ICMP)** me sirve para verificar que NAT está traduciendo las direcciones correctamente, pero no me muestra claramente cómo se asignan los puertos.
En cambio, con **Telnet (TCP)** puedo ver cómo **PAT asigna puertos diferentes a cada PC**, lo que me permite confirmar que la traducción está funcionando bien.
Como PAT usa **puertos diferentes para cada conexión TCP**, Telnet es la mejor opción para visualizar cómo PAT asigna puertos a cada conexión en **show ip nat translations**.

Diferencia entre NAT Estático, NAT Dinámico y PAT

Tipo de NAT	¿Cómo funciona?	Ejemplo
NAT Estático	Asigna una IP pública fija a una IP privada específica.	ip nat inside source static 10.1.0.2 172.22.34.124
NAT Dinámico	Usa un **pool** de IPs públicas y las asigna a IPs privadas cuando es necesario.	ip nat inside source list 1 pool MiPool
PAT (NAT Sobrecargado)	Traduce **varias IPs privadas** a **una sola IP pública**, diferenciando por puertos.	ip nat inside source list 1 interface GigabitEthernet0/1 overload

Resumen Final

NAT Estático: PC1 (10.1.0.2) tenía una IP pública fija (172.22.34.124).
NAT Dinámico: PC2 y PC3 (10.1.0.3 y 10.1.0.4) usaban la IP pública 172.22.34.123 de manera dinámica.
PAT (Sobrecarga): Todos los PCs compartieron la IP pública 172.22.34.123 usando diferentes puertos.

Con esto, hemos configurado correctamente el router Cisco para que los PCs accedan a Internet con diferentes métodos de NAT.

Nota: Dado que **Cisco Packet Tracer no simula Internet real**, solo podemos comprobar la traducción de direcciones con ping, pero en un entorno real podríamos verificarlo con protocolos TCP/UDP o Telnet.

Bibliografía

- Cisco. (2023). Configuración de Traducción de dirección de red
- Milvus . (2023). Como configurar el NAT en el Ruteador Cisco