UCUENCA

UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA

COMPUTACIÓN

Práctica 12 - Servicio NAT Network Address Translation

Integrantes:

Ledesma Fabián

Macas Kelly

Mendoza Bryan

Quizhpi Luis

Romero David

Asignatura: Redes de Computadoras

Docente: Ing. Raúl Ortiz, Ing. Andrea Mory

Fecha de entrega: 15/07/2025

Jefe de laboratorio	Ing. Raúl Ortiz Gaona PhD
Técnico de Laboratorio	Ing. Andrea Mory
Práctica # 13	Listas de Control de Acceso

1. ANTECEDENTES

Se puede diseñar una red y asignar direcciones IP privadas con toda libertad, pero los hosts no pueden navegar en Internet con una dirección IP privada. Para que se lo pueda hacer, es necesario que el enrutador de la red LAN que está conectada a Internet, le asigne al host una dirección IP pública. Esta tarea se lo hace a través del servicio NAT Network Address Translation.

2. OBJETIVOS

El objetivo de la práctica es el siguiente:
1. Configurar en el enrutador el servicio NAT.

3. EQUIPO Y MATERIALES

2 ruteadores
2 switches
4 PCs
6 cables directos
1 cable cruzado
1 cable de consola

4. DISEÑO DE LA RED CON MÁSCARA DE SUBRED DE LONGITUD FIJA

Datos:
Se tiene una red LAN con dirección de red IP privada 192.168.0.0
El servidor al que se desea acceder y que está en Internet tiene la dirección pública 172.100.0.2

5. INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS

1. Conectar los equipos como se indica en la Figura 1.
2. Configurar las PCs.
3. Configurar las interfaces de red de los enrutadores.
4. Configurar enrutamiento dinámico RIP en los enrutadores
5. Configurar el servicio NAT en el enrutador R1

```
Router(config)# access-list 1 permit 192.168.0.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface gigabitEthernet 0/1 overload
Router(config)# interface gigabitEthernet 0/0
```

```
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip nat outside
Router(config-if)# exit
```

6. Comprobar en las PCs si se asignaron dinámicamente las direcciones IP
7. Comprobar la conectividad entre PCs

Luego, los estudiantes configurarán NAT con dos redes LAN conectadas al enrutador R1, con direcciones de red privadas clase A y B respectivamente

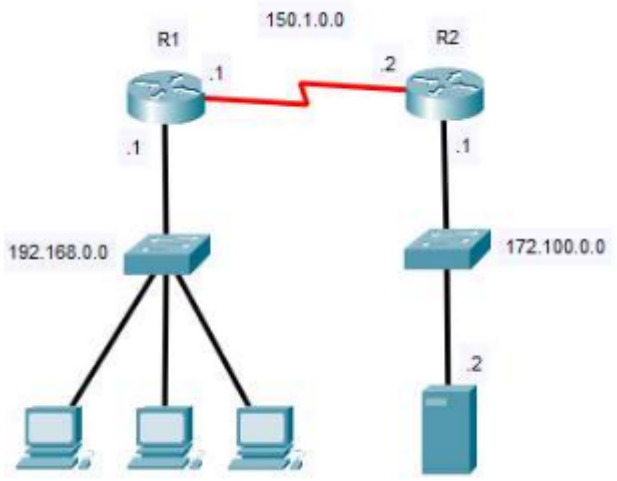

Figura 1. Topología de red

6. RESULTADOS OBTENIDOS

Esta práctica se realizó únicamente en el software Cisco Packet Tracer.

Primero se investigó sobre NAT y su funcionamiento. NAT significa traducción de direcciones de red. Es una técnica utilizada para permitir que múltiples dispositivos en una red privada compartan una única dirección IP pública al conectarse a Internet. NAT funciona traduciendo las direcciones IP privadas de los dispositivos internos a una dirección IP pública antes de que los paquetes salgan de la red.

Con ese pequeño contexto se procedió a realizar la práctica en Cisco Packet Tracer. Primero se realizó la topología pedida en la práctica. Se debe considerar que para la conexión de los routers por un medio WAN se tenía que agregar un puerto serial. Sabiendo eso se realizó la topología como se muestra en la Figura 2.

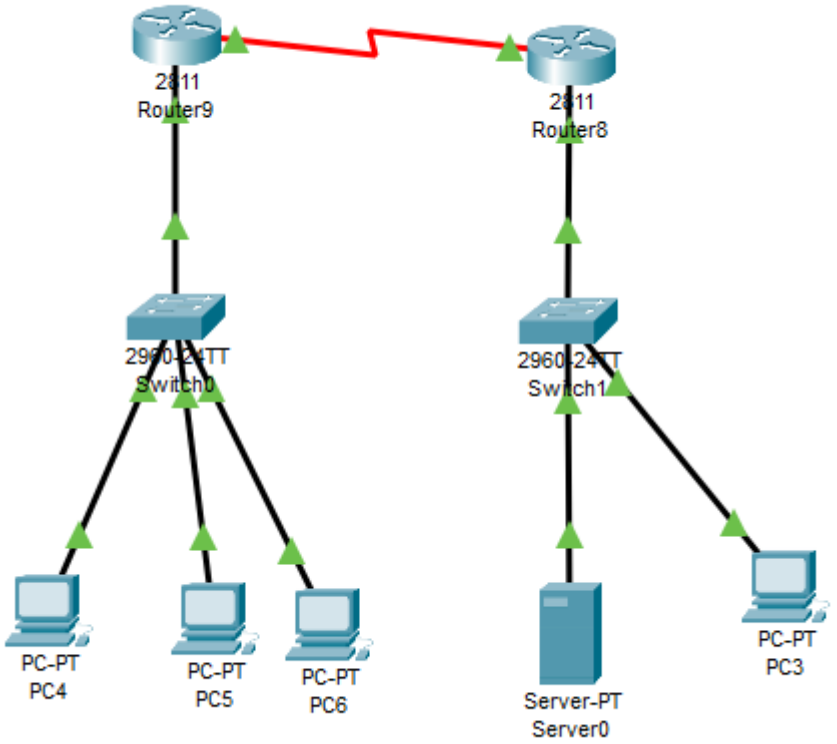

Figura 2. Topología creada en Cisco Packet Tracer

Ahora antes de ingresar los comandos se investigó un poco acerca de ellos.

- access-list 1 permit 192.168.0.0 0.0.0.255: Este comando primero crea una lista de control de acceso. También define la red interna que podrá ser traducida. El "0.0.0.255" es una wildcard mask que equivale a la máscara de subred /24. Permite cualquier host desde 192.168.0.0 – 192.168.0.255.
- ip nat inside source list 1 interface gigabitEthernet 0/1 overload: El comando activa NAT usando como criterio la ACL 1 recién creada. También tomará las direcciones que esen "dentro-inside" de la ACL y las traducirá a la dirección "afuera-outside" que posee la interfaz GigabitEthernet 0/1. Por último el comando también permite que muchos hosts internos compartan la misma dirección IP pública de Gi0/1 diferenciándose por sus números de puerto.

Al conocer mejor los comandos procedemos a configurar cada router:

Primer router

- Configuración de la 1ra interfaz - switch

```
Router>enable
Router#configure terminal
Router(config)#interface fa 0/0
```

```
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

- Configuración de la 2da interfaz - router

```
Router(config)#interface se 0/2/0
Router(config-if)#ip address 150.1.0.1 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Segundo router

- Configuración de la 1ra interfaz - switch

```
Router>enable
Router#configure terminal
Router(config)#interface fa 0/0
Router(config-if)#ip address  170.100.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

- Configuración de la 2da interfaz - router

```
Router(config)#interface se 0/2/0
Router(config-if)#ip address 150.1.0.2 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

A continuación, se configuró la NAT :

Primer router

```
Router(config)# access-list 1 permit 192.168.0.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface gigabitEthernet 0/1 overload
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip nat outside
Router(config-if)# exit
```

Por último configuramos RIP en ambos routers:

Primer router

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.0.0
Router(config-router)#network 150.1.0.0
Router(config-router)#exit
```

Segundo router

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 170.100.0.0
Router(config-router)#network 150.1.0.0
Router(config-router)#exit
```

A continuación, se realizó la configuración de las IP's respectivas por cada una de las computadoras y servidores.

- Computadoras correspondientes a la red 192.168.0.0

  IP: 192.168.0.2
  Máscara: 255.255.255.0
  Gateway: 192.168.0.1

  IP: 192.168.0.3
  Máscara: 255.255.255.0
  Gateway: 192.168.0.1

  IP: 192.168.0.4
  Máscara: 255.255.255.0
  Gateway: 192.168.0.1

- Computadora y Server correspondientes a la red 170.100.0.0

  IP: 172.100.0.10
  Máscara: 255.255.255.0
  Gateway: 172.100.0.1

  IP: 172.100.0.20
  Máscara: 255.255.255.0
  Gateway: 172.100.0.1

Para verificar las conexiones y configuraciones realizadas se realizó un ping entre las computadoras y el server como se puede ver en las imágenes 3, 4 y 5.

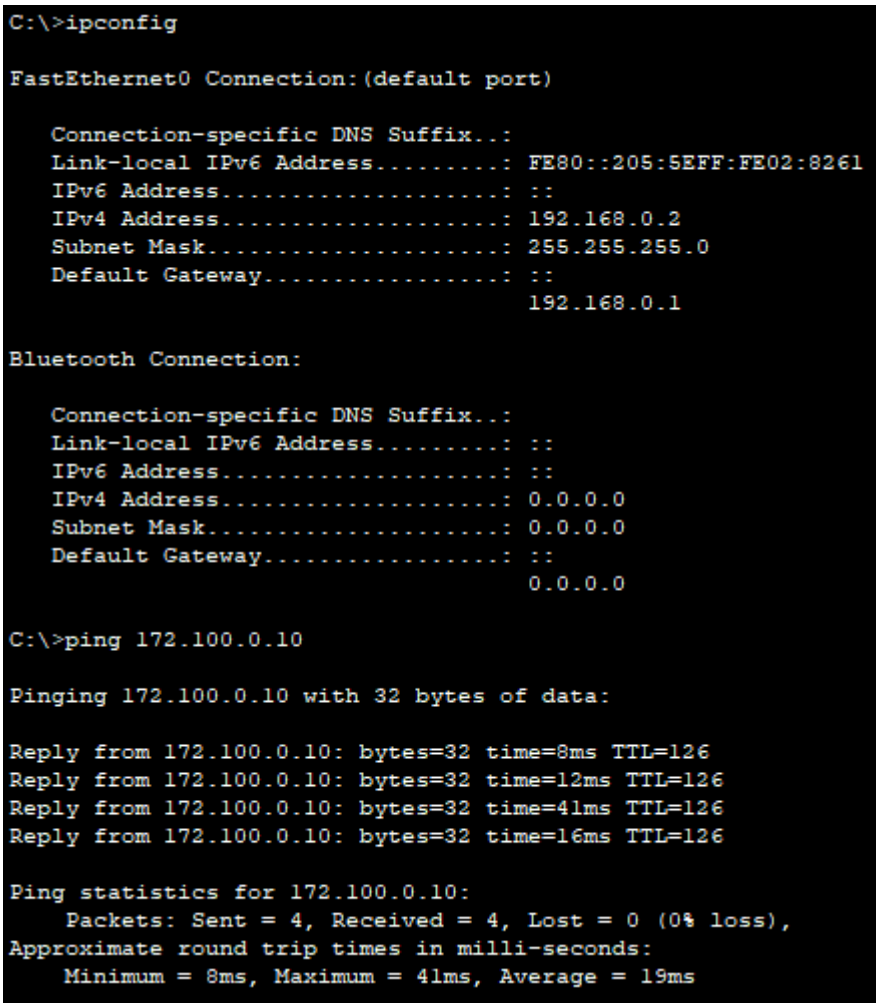

Figura 3. Comprobación de la conexión entre host 192.168.0.2 con server

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:C7FF:FE15:6705
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.0.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 172.100.0.10

Pinging 172.100.0.10 with 32 bytes of data:

Reply from 172.100.0.10: bytes=32 time=1ms TTL=126
Reply from 172.100.0.10: bytes=32 time=9ms TTL=126
Reply from 172.100.0.10: bytes=32 time=37ms TTL=126
Reply from 172.100.0.10: bytes=32 time=13ms TTL=126

Ping statistics for 172.100.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 37ms, Average = 15ms
```

Figura 4. Comprobación de la conexión entre host 192.168.0.3 con server

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2D0:BCFF:FE9B:81A0
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.4
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.0.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 172.100.0.10

Pinging 172.100.0.10 with 32 bytes of data:

Reply from 172.100.0.10: bytes=32 time=1ms TTL=126
Reply from 172.100.0.10: bytes=32 time=1ms TTL=126
Reply from 172.100.0.10: bytes=32 time=9ms TTL=126
Reply from 172.100.0.10: bytes=32 time=13ms TTL=126

Ping statistics for 172.100.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 6ms
```

Figura 5. Comprobación de la conexión entre host 192.168.0.4 con server

Ahora que se comprobó que las conexiones están bien podemos probar si alguna de las computadoras tiene accesos a la red. Como se ve en la figura 6 se tiene que activar el servicio HTTP en el server para que provea a las computadoras.

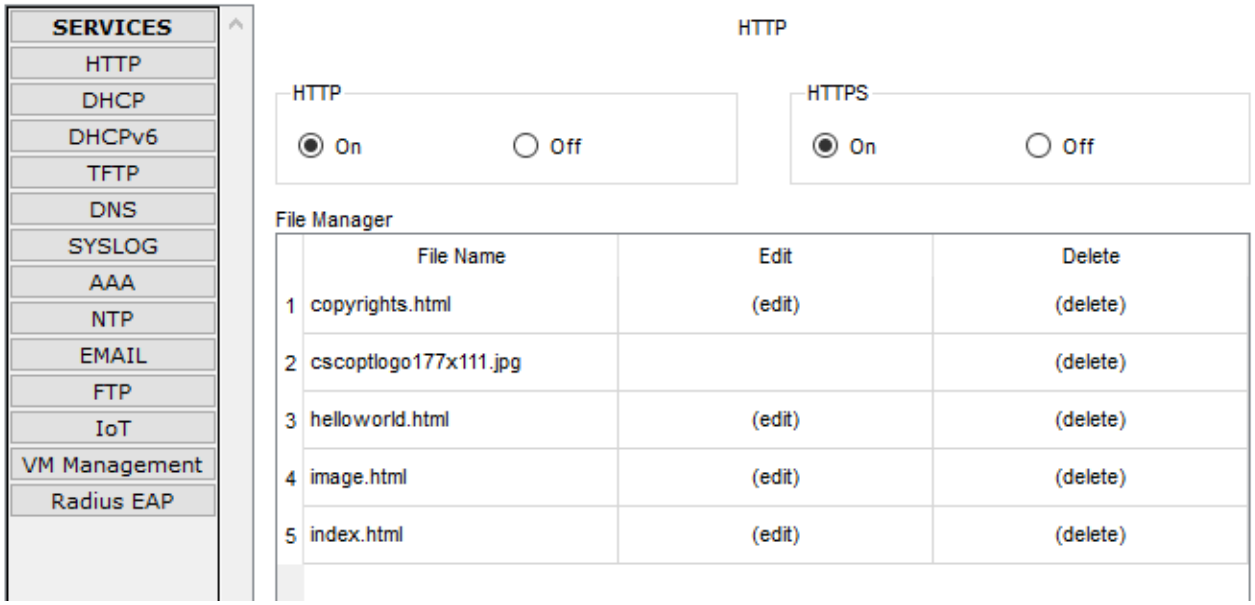

Figura 6. Activación de servicio HTTP

Después de activar el servicio se ingresa en un navegador de una computadora e ingresamos la dirección del server. Si la NAT fue configurada correctamente nos aparecerá una página provista por Packet Tracer para hacer este tipo de pruebas como se observa en la figura 7.

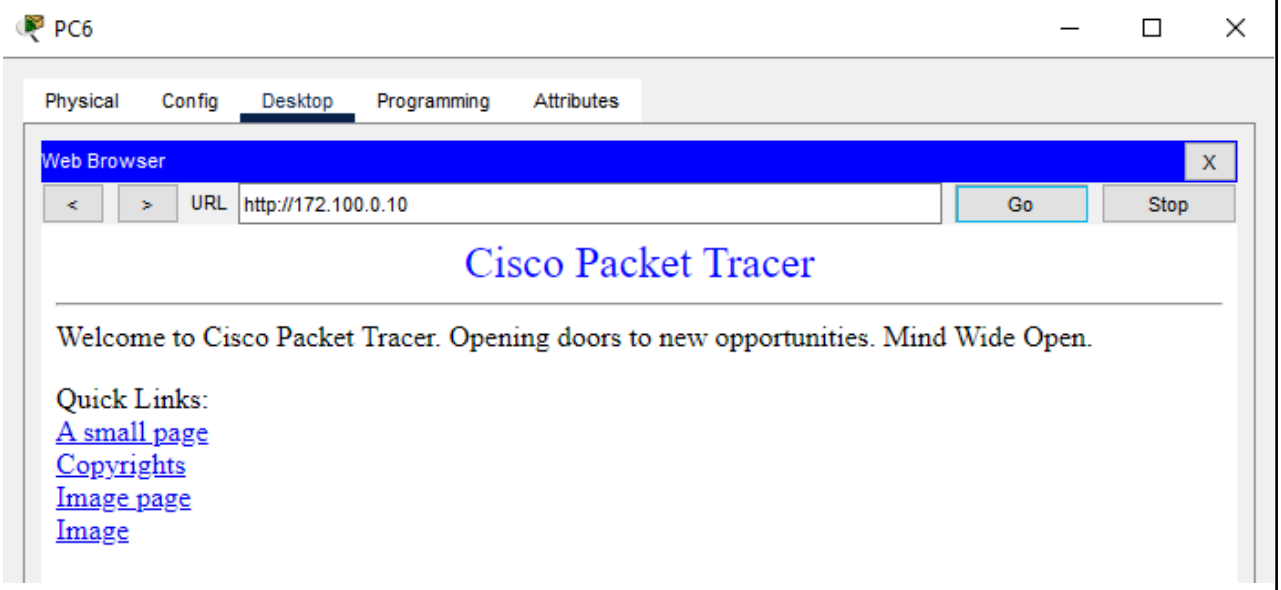

Figura 7. Ingreso a una página web desde una PC.

7. CONCLUSIONES

- Se comprendió la importancia de NAT como solución al agotamiento de direcciones IPv4, permitiendo que redes privadas accedan a Internet sin necesidad de direcciones públicas para cada dispositivo.
- Cisco Packet Tracer demostró ser una herramienta efectiva para simular el funcionamiento de NAT y comprender su aplicación práctica en redes empresariales.

8. RECOMENDACIONES

- Asegurarse de identificar correctamente las interfaces "inside" (red privada) y "outside" (red pública) para evitar errores en la traducción.
- Mantener un registro de las listas de acceso y configuraciones NAT implementadas para facilitar el mantenimiento futuro.
- Diseñar cuidadosamente el esquema de direcciones IP para evitar conflictos entre redes privadas y públicas.
- Experimentar con diferentes topologías de red para comprender mejor las aplicaciones de NAT en distintos entornos.

9. FUENTES DE INFORMACIÓN