

PRÁCTICA: NAT(Network Address Translation)

FECHA:08/05/2024

GRUPO: 7CM2

NOMBRE DEL EQUIPO: Gepetos

Integrantes:

Torres Abonce Luis Miguel
Salazar Carreón Jeshua Jonathan

Topología Propuesta configuración de la NAT

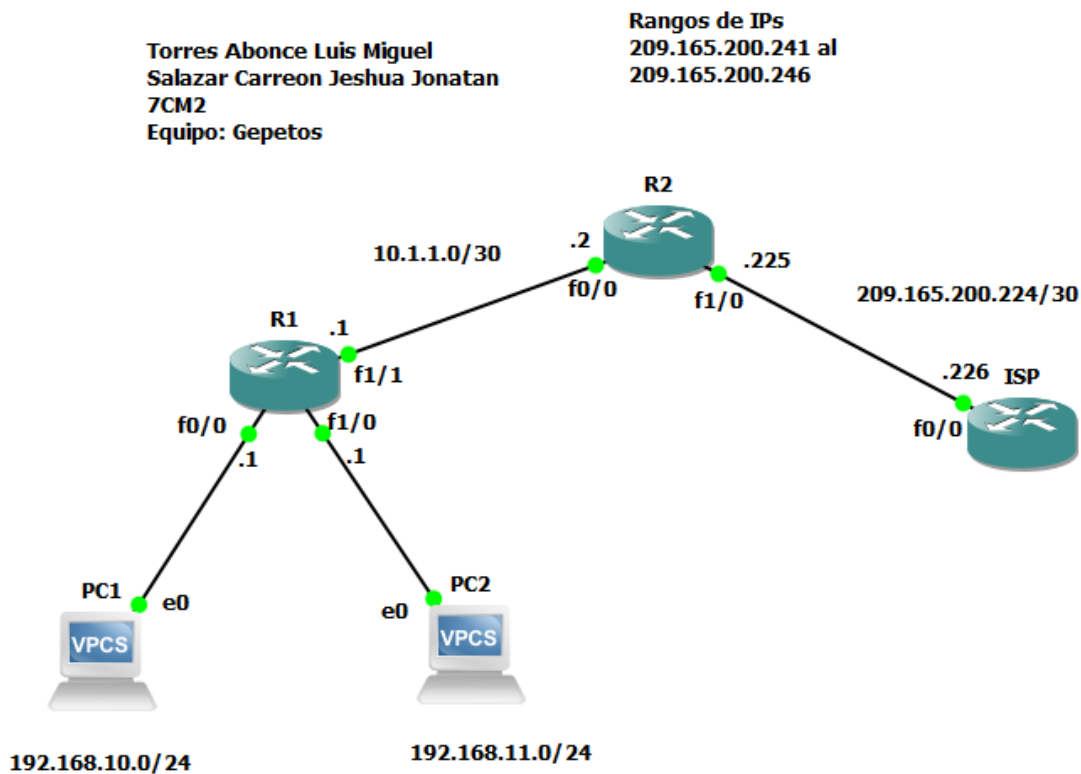


TABLA DE DIRECCIONAMIENTO

Dispositivo	Interface	Dirección IP	Máscara de subred	Puerta de enlace predeterminada
R1	f0/0	192.168.10.1	/24	
	f1/0	192.168.11.1	/24	
	f1/1	10.1.1.1	/30	
R2	f0/0	10.1.1.2	/30	
	f1/0	209.165.200.225	/30	
ISP	G0/0	209.165.200.226	/30	

Configuramos el enrutamiento estático en ISP:

```
ISP(config)#ip route 209.165.200.240 255.255.255.252 209.165.200.225
ISP(config)#end
ISP#
```

Configuramos router 2:

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#rout
R2(config)#router os
R2(config)#router ospf 1
R2(config-router)#netwo
R2(config-router)#network 10.1.1.0 0.0.0.3 ar
R2(config-router)#network 10.1.1.0 0.0.0.3 area 0
R2(config-router)#network 192.168.10.0 0.0.0.255 area 0
R2(config-router)#network 192.168.11.0 0.0.0.255 area 0
R2(config-router)#network 209.165.200.224 0.0.0.3 area 0
R2(config-router)#default-information originate always
R2(config-router)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
R2(config)#$ MI_NAT_POOL 209.200.241 209.165.200.246 netmask 255.255.255.248
R2(config)#ip nat pool MI_NAT_POOL 209.165.200.241 209.165.200.246 netmask 255$
R2(config)#ip access-list extended NAT
R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

LIGAMOS POOL CON ACCES-LIST:

```
R2(config)#ip nat inside source list NAT pool MI_NAT_POOL
```

DEFINIMOS LA PARTE INTERNA Y EXTERNA DE NUESTRA NAT:

```
R2(config)#ip nat inside source list NAT pool MI_NAT_POOL
R2(config)#int f0/0
R2(config-if)#ip nat inside
R2(config-if)#int f1/0
R2(config-if)#ip nat outside
R2(config-if)#exit
```

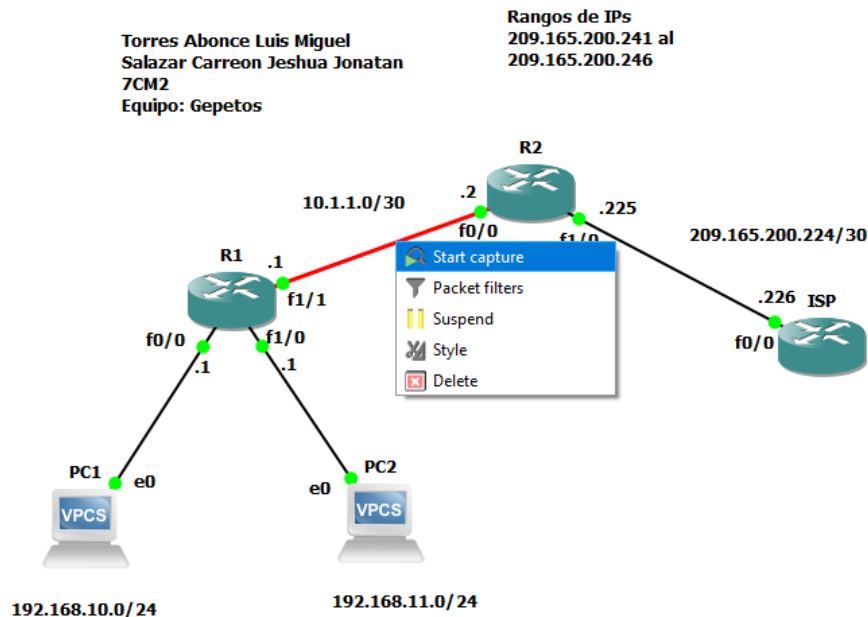
Al hacer un ping podemos ver las traducciones con el comando:

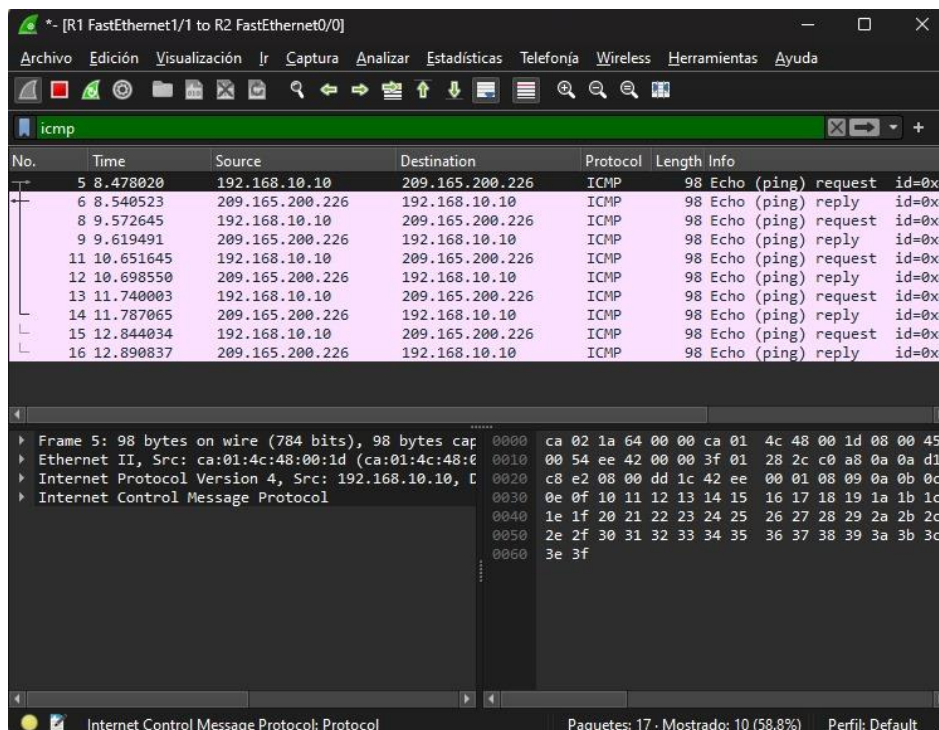
```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.241:18449 192.168.10.10:18449 209.165.200.226:18449 209.165.200.226:18449
icmp 209.165.200.241:18961 192.168.10.10:18961 209.165.200.226:18961 209.165.200.226:18961
icmp 209.165.200.241:19473 192.168.10.10:19473 209.165.200.226:19473 209.165.200.226:19473
icmp 209.165.200.241:19729 192.168.10.10:19729 209.165.200.226:19729 209.165.200.226:19729
icmp 209.165.200.241:19985 192.168.10.10:19985 209.165.200.226:19985 209.165.200.226:19985
--- 209.165.200.241      192.168.10.10      ---                ---
```

Pasamos a pc1 donde hacemos ping a 200.165.200.226 PC1> ping 209.165.200.226 -t:

```
PC1> ping 209.165.200.226
209.165.200.226 icmp_seq=1 timeout
209.165.200.226 icmp_seq=2 timeout
84 bytes from 209.165.200.226 icmp_seq=3 ttl=253 time=75.354 ms
84 bytes from 209.165.200.226 icmp_seq=4 ttl=253 time=75.908 ms
84 bytes from 209.165.200.226 icmp_seq=5 ttl=253 time=76.017 ms
```

Habilitamos wireshark en la interfaz del R1 y R2 para verificar que la NAT esté trabajando. En wireshark filtramos el tráfico por paquete ICMP.



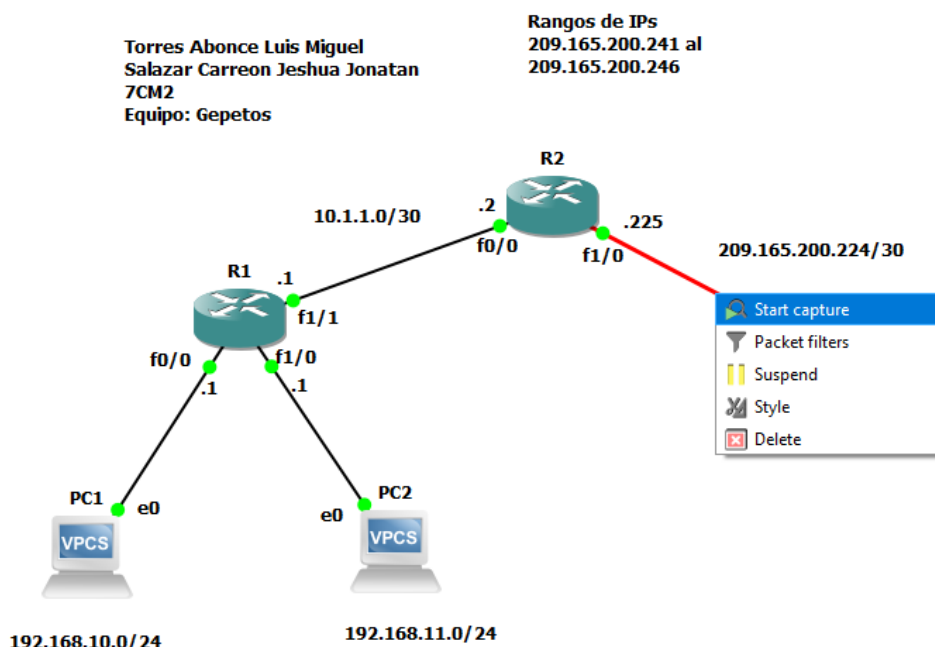


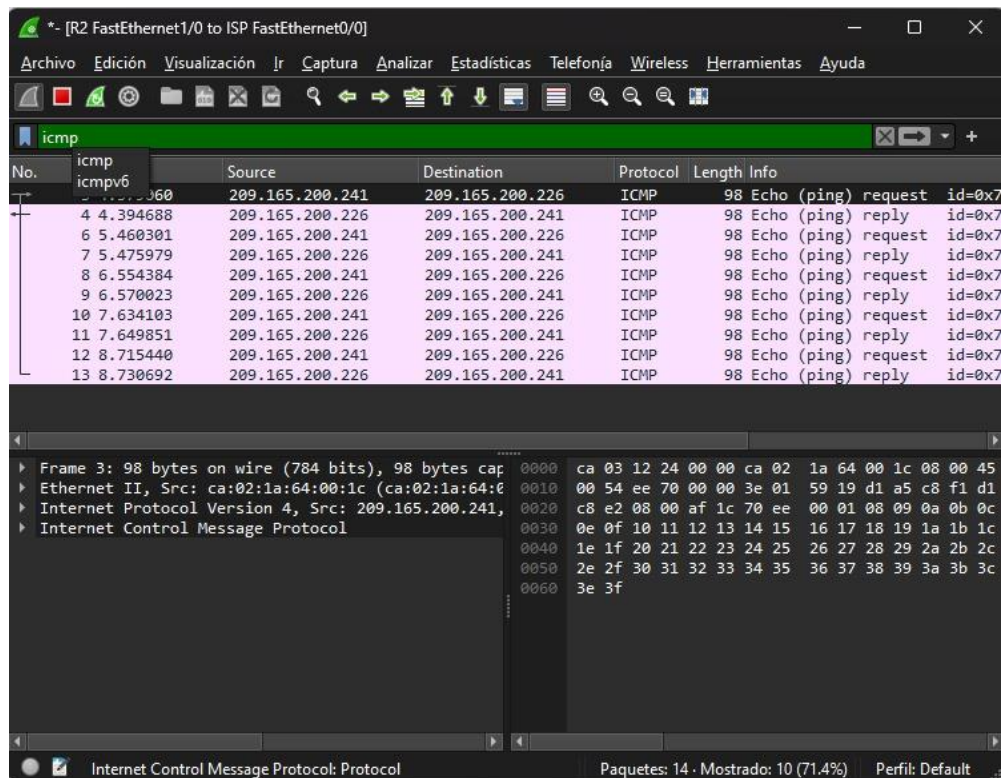
No.	Time	Source	Destination	Protocol	Length	Info
5	8.478020	192.168.10.10	209.165.200.226	ICMP	98	Echo (ping) request id=0x4
6	8.540523	209.165.200.226	192.168.10.10	ICMP	98	Echo (ping) reply id=0x4
8	9.572645	192.168.10.10	209.165.200.226	ICMP	98	Echo (ping) request id=0x4
9	9.619491	209.165.200.226	192.168.10.10	ICMP	98	Echo (ping) reply id=0x4
11	10.651645	192.168.10.10	209.165.200.226	ICMP	98	Echo (ping) request id=0x4
12	10.698550	209.165.200.226	192.168.10.10	ICMP	98	Echo (ping) reply id=0x4
13	11.740003	192.168.10.10	209.165.200.226	ICMP	98	Echo (ping) request id=0x4
14	11.787065	209.165.200.226	192.168.10.10	ICMP	98	Echo (ping) reply id=0x4
15	12.844034	192.168.10.10	209.165.200.226	ICMP	98	Echo (ping) request id=0x4
16	12.890837	209.165.200.226	192.168.10.10	ICMP	98	Echo (ping) reply id=0x4

Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 Ethernet II, Src: ca:01:4c:48:00:1d (ca:01:4c:48:00:1d), Dst: 08:00:0c:2c:c0:a8
 Internet Protocol Version 4, Src: 192.168.10.10, Destination: 209.165.200.226
 Internet Control Message Protocol

Observamos que las direcciones IP son las que asignamos en el rango, de la 192.168.10.11 hasta la 209.165.200.226 y le está contestando 209.165.200.226 a la 192.068.10.11

Ahora vamos a poner el wireshark después del ISP PARA VERIFICAR EL CAMBIO DE IP





No.	icmp	Source	Destination	Protocol	Length	Info
4	icmpv6	209.165.200.241	209.165.200.226	ICMP	98	Echo (ping) request id=0x7
5	icmp	209.165.200.226	209.165.200.241	ICMP	98	Echo (ping) reply id=0x7
6	icmp	209.165.200.241	209.165.200.226	ICMP	98	Echo (ping) request id=0x7
7	icmp	209.165.200.226	209.165.200.241	ICMP	98	Echo (ping) reply id=0x7
8	icmp	209.165.200.241	209.165.200.226	ICMP	98	Echo (ping) request id=0x7
9	icmp	209.165.200.226	209.165.200.241	ICMP	98	Echo (ping) reply id=0x7
10	icmp	209.165.200.241	209.165.200.226	ICMP	98	Echo (ping) request id=0x7
11	icmp	209.165.200.226	209.165.200.241	ICMP	98	Echo (ping) reply id=0x7
12	icmp	209.165.200.241	209.165.200.226	ICMP	98	Echo (ping) request id=0x7
13	icmp	209.165.200.226	209.165.200.241	ICMP	98	Echo (ping) reply id=0x7

Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 Ethernet II, Src: ca:02:1a:64:00:1c (ca:02:1a:64:00:1c), Dst: 08:00:00:00:00:00
 Internet Protocol Version 4, Src: 209.165.200.241, Destination: 209.165.200.226
 Internet Control Message Protocol

De Esta manera verificamos que nuestro Servidor NAT está realizando su función de traducir las IP privadas en IP públicas.

Conclusiones:

En esta práctica nos permitió comprender y verificar cómo se realiza la traducción de direcciones IP privadas a direcciones IP públicas. Durante la práctica, configuramos dispositivos y empleamos herramientas como Wireshark para observar directamente el proceso de traducción, lo que permitió validar el funcionamiento correcto del NAT en un entorno controlado. Esto es crucial para la gestión de redes ya que el NAT permite que múltiples dispositivos en una red privada accedan a internet utilizando una única dirección IP pública, optimizando el uso de las direcciones IP disponibles y aumentando la seguridad al ocultar las direcciones internas.