



INSTITUTO POLITÉCNICO
NACIONAL



ESCUELA SUPERIOR DE CÓMPUTO

ADMINISTRACIÓN DE SERVICIOS EN RED

Práctica 11

Autor:

Hernández Castellanos César Uriel
Pimentel González Carlos

Docente:

Henestrosa Carrasco Leticia

Ingeniería en Sistemas Computacionales

27 de Septiembre de 2019

Índice

1.2	Introducción.	3
2.	Objetivos	3
3.	Desarrollo.	3
3.1.	Aislar los problemas.	3
3.2.	Resolver los problemas de configuración NAT.	4
3.3.	Verificar la conectividad.	7
4.	Resultado final del test	9
5.	Conclusiones	10
6.	Referencias	10

1. Introducción.

El crecimiento de la cantidad de dispositivos que usan internet ha hecho prácticamente la cantidad de IPv4 disponibles, haya sido superada hace mucho. Para solucionar este problema tenemos IPv6 pero la dificultad que implica cambiar la configuración de las redes actuales en el mundo, es muy grande. La otra solución que se planteo, es NAT o Network Address Translation, la cual nos permite tener diferentes IPs de manera interna (privada) y poder comunicarnos externamente mediante una IP externa (publica). NAT tiene 3 formas de usarse, las cuales pueden ser estática, la cual traduce una dirección privada a una publica, dinámica la cual traduce varias direcciones privadas a varias publicas, y PAT, la cual nos permite utilizar los puertos para asignar varias IPs privadas a una única IP publica.

En esta práctica vemos un escenario en el cual tenemos que solucionar los diferentes problemas que se presentan en la topología presentada, pero sobre configuraciones de NAT.

2. Objetivos

Los objetivos de la práctica, como tal es la resolución de problemas en una red configurada con NAT. Tareas como identificar y aislar problemas, verificar la conectividad correctamente, es decir, que lo planteado en el escenario, sea lo que esta configurado. Y finalmente poder resolver estos problemas. En resumen, estos serian nuestros 3 objetivos principales.

- Aislar problemas
- Resolución de problemas de la configuración NAT
- Verificar conectividad

3. Desarrollo.

3.1. Aislar los problemas.

Haga ping al Servidor1 desde PC1, PC2, L1, L2 y el R2. Registre cada ping correcto. Haga ping a cualquier otra máquina según sea necesario.

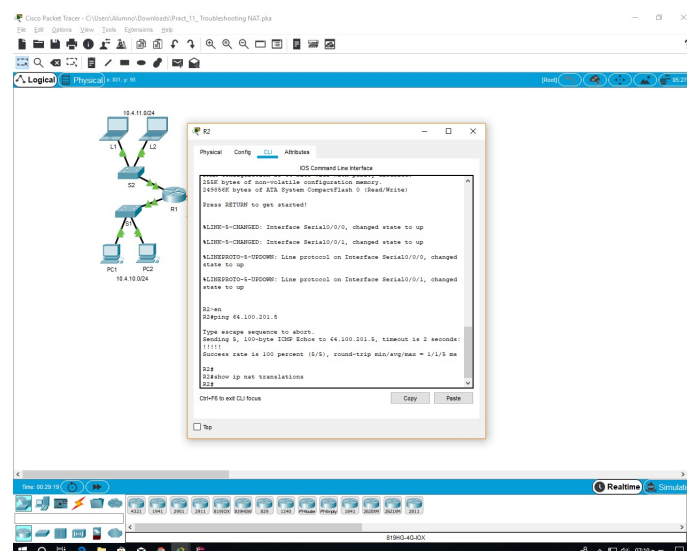


Figura 1: Ping desde R2 al Servidor1

Se comprobó que existiera conexión entre PC1, PC2, L1 y L2 al servidor 1, por lo que se omitiran las capturas.

3.2. Resolver los problemas de configuración NAT.

Ver las traducciones NAT en R2

```
1/4/11 ms

R2#sh
R2#show ip
R2#show ip nat
R2#show ip nat tr
R2#show ip nat translations
R2#
```

Figura 2: Traducciones en R2

Mostrar la configuración en ejecución en el R2.

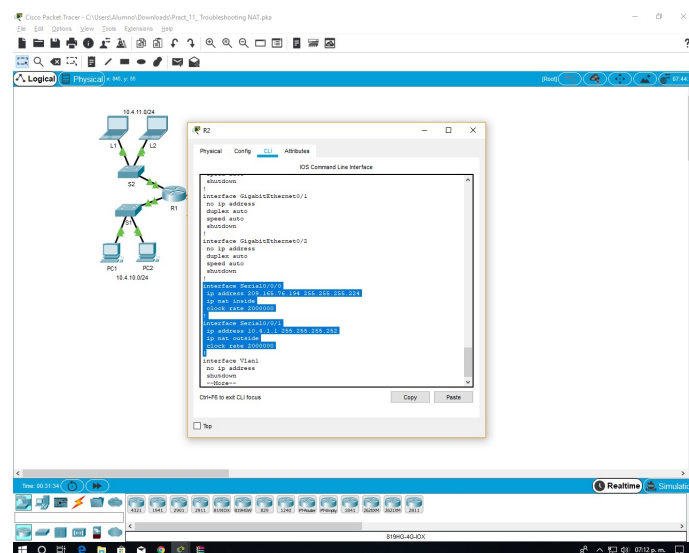


Figura 3: Configuración actual de R2

Asignando a los comandos ip nat inside e ip nat outside a los puertos correctos.

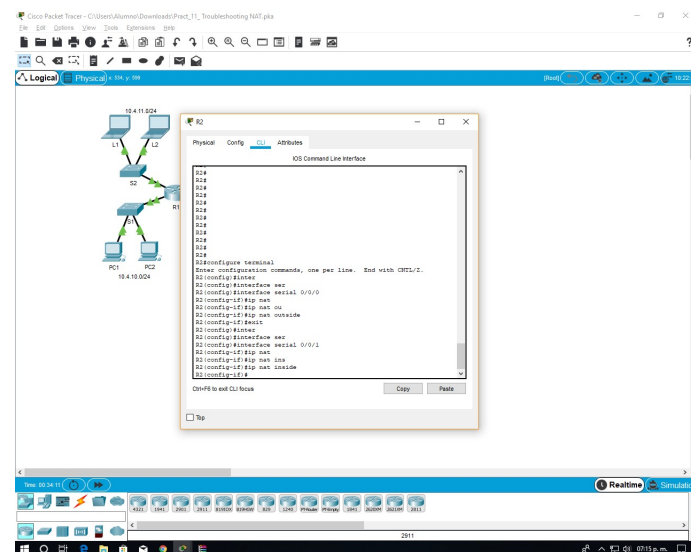


Figura 4: Corrección de interfaces

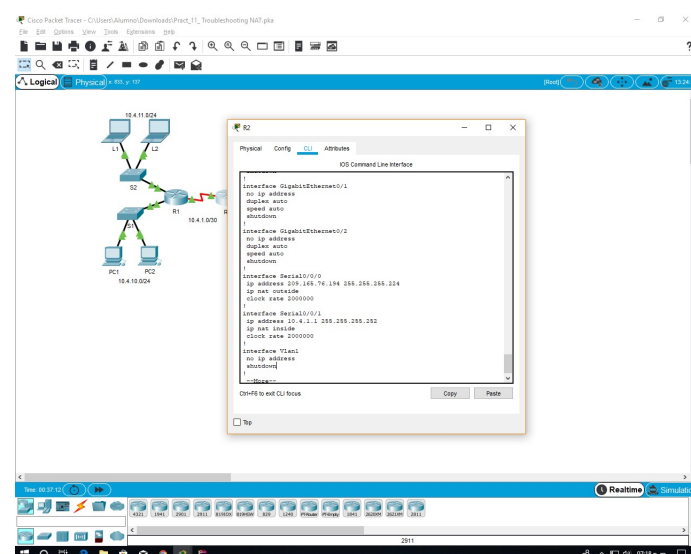


Figura 5: Verificación de la corrección

Hacer ping al Servidor1 desde PC1, PC2, L1, L2 y el R2.

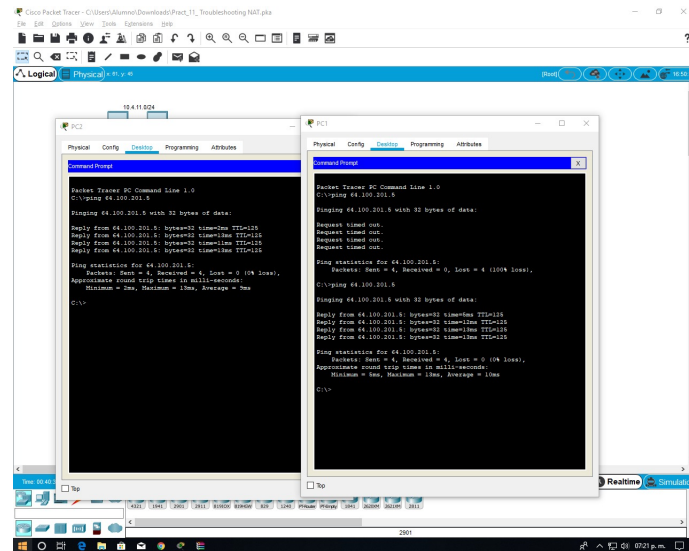


Figura 6: Ping desde PC1 Y PC2 al servidor

Ver las traducciones NAT en el R2.

```
R2#sh
R2#show ip nat
R2#show ip nat tr
R2#show ip nat translations
R2#show ip nat translations
Pro Inside global      Inside local      Outside local
-----
Outside global
icmp 209.165.76.196:10 10.4.10.2:10      64.100.201.5:10
64.100.201.5:10
icmp 209.165.76.196:11 10.4.10.2:11      64.100.201.5:11
64.100.201.5:11
icmp 209.165.76.196:12 10.4.10.2:12      64.100.201.5:12
64.100.201.5:12
icmp 209.165.76.196:9  10.4.10.2:9       64.100.201.5:9
64.100.201.5:9
```

Figura 7: Traducciones en R2

Mostrar la lista de acceso 101 en el R2.

```
shutdown
!
ip nat pool R2POOL 209.165.76.195 209.165.76.223 netmask
255.255.255.224
ip nat inside source list 101 pool R2POOL
ip classless
ip route 10.0.0.0 255.0.0.0 10.4.1.2
ip route 0.0.0.0 0.0.0.0 209.165.76.193
!
ip flow-export version 9
!
!
access-list 101 permit ip 10.4.10.0 0.0.0.255 any
!
```

Figura 8: Lista de acceso 101

Corregir la lista de acceso.

10.4.00001010.0 10.4.10.0/24

10.4.00001011.0 10.4.11.0/24

10.4.00001010.0 10.4.10.0/23

255.255.255.255

255.255.254.0

0.0.1.255

```
R2(config)#access-list 101 permit ip 10.4.10.0 0.0.1.255 ?
  A.B.C.D  Destination address
  any      Any destination host
  host      A single destination host
R2(config)#access-list 101 permit ip 10.4.10.0 0.0.1.255 any
```

Figura 9: Corrección de la lista de acceso

3.3. Verificar la conectividad.

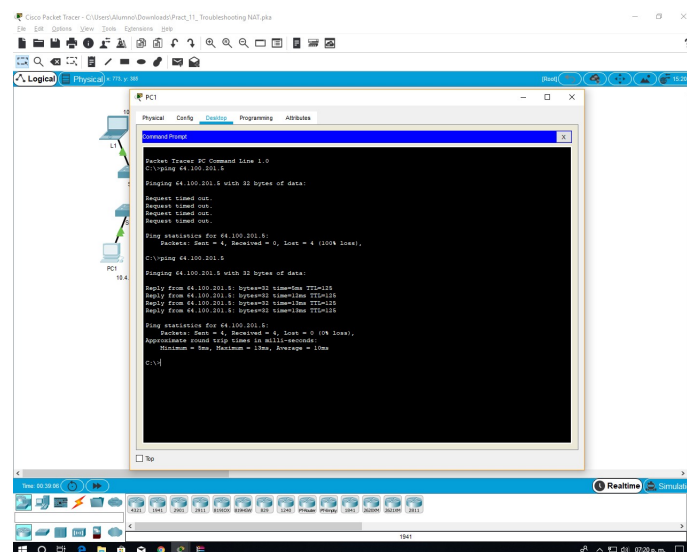
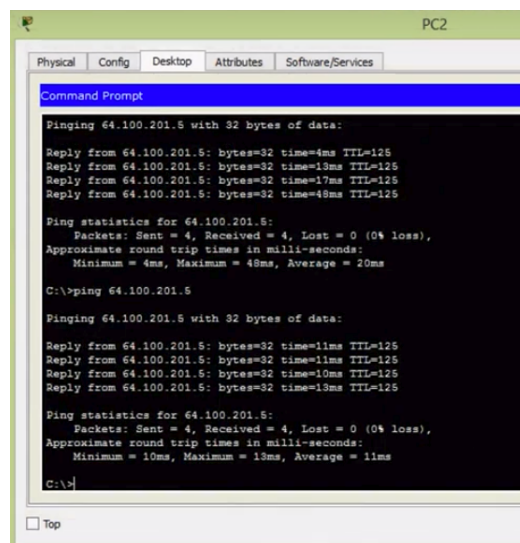


Figura 10: Conexión desde PC1 al servidor



```
PC2
Physical Config Desktop Attributes Software/Services
Command Prompt

Pinging 64.100.201.5 with 32 bytes of data:

Reply from 64.100.201.5: bytes=32 time=4ms TTL=125
Reply from 64.100.201.5: bytes=32 time=13ms TTL=125
Reply from 64.100.201.5: bytes=32 time=17ms TTL=125
Reply from 64.100.201.5: bytes=32 time=48ms TTL=125

Ping statistics for 64.100.201.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 48ms, Average = 20ms

C:\>ping 64.100.201.5

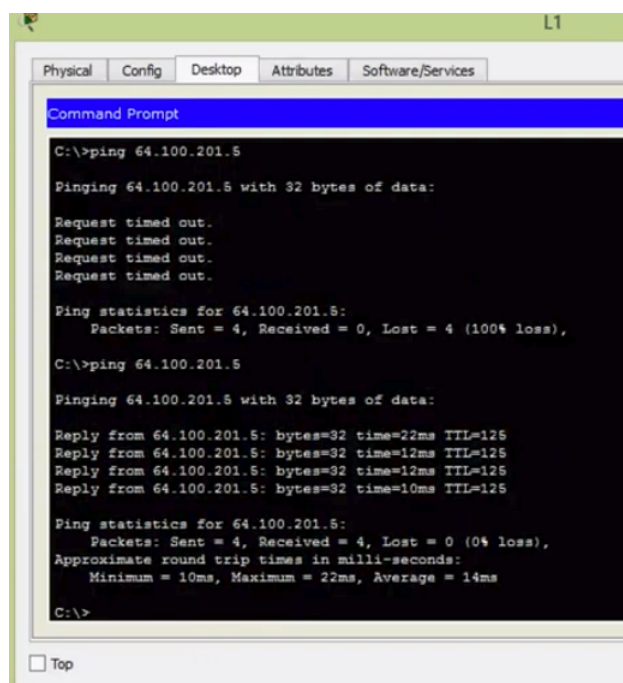
Pinging 64.100.201.5 with 32 bytes of data:

Reply from 64.100.201.5: bytes=32 time=11ms TTL=125
Reply from 64.100.201.5: bytes=32 time=11ms TTL=125
Reply from 64.100.201.5: bytes=32 time=10ms TTL=125
Reply from 64.100.201.5: bytes=32 time=13ms TTL=125

Ping statistics for 64.100.201.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 13ms, Average = 11ms

C:\>
```

Figura 11: Conexión desde PC2 al servidor



```
L1
Physical Config Desktop Attributes Software/Services
Command Prompt

C:\>ping 64.100.201.5

Pinging 64.100.201.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 64.100.201.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 64.100.201.5

Pinging 64.100.201.5 with 32 bytes of data:

Reply from 64.100.201.5: bytes=32 time=22ms TTL=125
Reply from 64.100.201.5: bytes=32 time=12ms TTL=125
Reply from 64.100.201.5: bytes=32 time=12ms TTL=125
Reply from 64.100.201.5: bytes=32 time=10ms TTL=125

Ping statistics for 64.100.201.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 22ms, Average = 14ms

C:\>
```

Figura 12: Conexión desde L1 al servidor


```

Ping statistics for 64.100.201.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 64.100.201.5

Pinging 64.100.201.5 with 32 bytes of data:

Reply from 64.100.201.5: bytes=32 time=11ms TTL=125
Reply from 64.100.201.5: bytes=32 time=11ms TTL=125
Reply from 64.100.201.5: bytes=32 time=11ms TTL=125
Reply from 64.100.201.5: bytes=32 time=12ms TTL=125

Ping statistics for 64.100.201.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 12ms, Average = 11ms

```

Figura 13: Conexión desde L2 al servidor

```

R2#show ip nat tr
R2#show ip nat translations

```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.76.200:21	10.4.10.1:21	64.100.201.5:21	64.100.201.5:21
icmp	209.165.76.200:22	10.4.10.1:22	64.100.201.5:22	64.100.201.5:22
icmp	209.165.76.200:23	10.4.10.1:23	64.100.201.5:23	64.100.201.5:23
icmp	209.165.76.200:24	10.4.10.1:24	64.100.201.5:24	64.100.201.5:24
icmp	209.165.76.201:17	10.4.10.2:17	64.100.201.5:17	64.100.201.5:17
icmp	209.165.76.201:18	10.4.10.2:18	64.100.201.5:18	64.100.201.5:18
icmp	209.165.76.201:19	10.4.10.2:19	64.100.201.5:19	64.100.201.5:19
icmp	209.165.76.201:20	10.4.10.2:20	64.100.201.5:20	64.100.201.5:20
icmp	209.165.76.202:17	10.4.11.1:17	64.100.201.5:17	64.100.201.5:17
icmp	209.165.76.202:18	10.4.11.1:18	64.100.201.5:18	64.100.201.5:18
icmp	209.165.76.202:19	10.4.11.1:19	64.100.201.5:19	64.100.201.5:19
icmp	209.165.76.202:20	10.4.11.1:20	64.100.201.5:20	64.100.201.5:20
icmp	209.165.76.203:13	10.4.11.2:13	64.100.201.5:13	64.100.201.5:13
icmp	209.165.76.203:14	10.4.11.2:14	64.100.201.5:14	64.100.201.5:14
icmp	209.165.76.203:15	10.4.11.2:15	64.100.201.5:15	64.100.201.5:15
icmp	209.165.76.203:16	10.4.11.2:16	64.100.201.5:16	64.100.201.5:16

Figura 14: Traducciones en R2

4. Resultado final del test

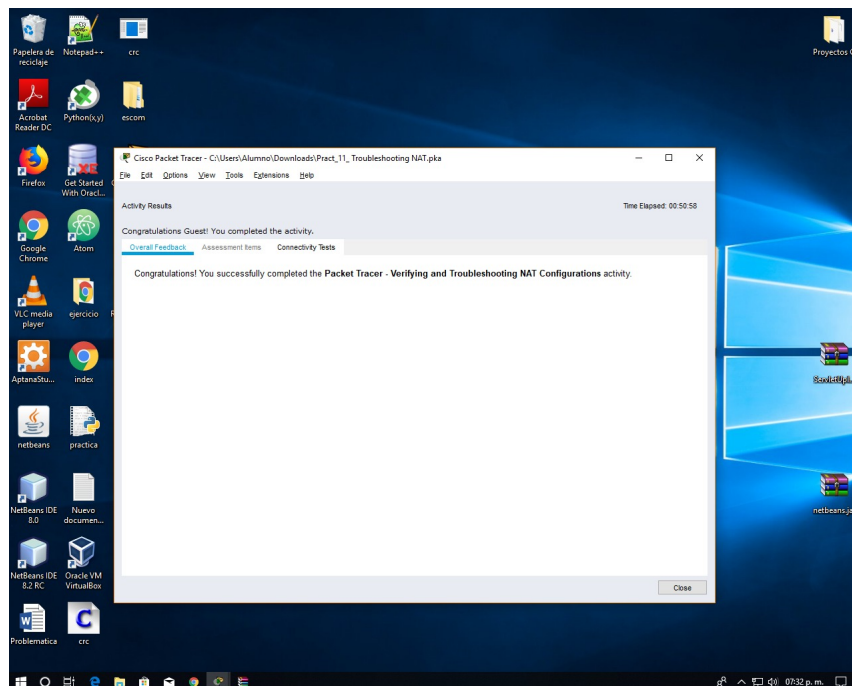


Figura 15: Resultado final

5. Conclusiones

Como podemos ver, el uso de NAT es algo que esta extendido ya en nuestros hogares, así como en redes privadas de empresas. Esto debido a que es necesario ahorrar direcciones IPv4. De esta manera una ISP, usando PAT, puede tener bajo una sola dirección publica, miles de dispositivos privados los cuales tengan asignado un puerto únicamente. Esto permite como se menciona el ahorrar direcciones IPv4. Pero también es importante el hecho de que podemos usar NAT por seguridad. NAT también es usada para ocultar nuestra dirección, o direcciones de nuestra red privada detrás de otras direcciones IP que sean publicas. Por esto es importante saber el como es que se configuran NAT, así como poder resolver algún problema de configuración que pueda surgir con estas configuraciones en nuestra red.

6. Referencias

[1]Cisco Networking Academy Builds IT Skills Education For Future Careers”, Netacad.com, 2019. [Online]. Available: <https://www.netacad.com/es>. [Accessed: 27/09/19].