



Instituto Politécnico Nacional



Escuela Superior de Cómputo

Práctica 2_8 Configuring Static NAT

Materia:

Administración de servicios en red

Grupo:

4CV13

Profesor:

Henestrosa Carrasco Leticia

Integrantes: (*Equipo 1*)

Arévalo Andrade Miguel Ángel
Castro Cruces Jorge Eduardo
López Mares Irene Elizabeth
Pedroza García Rodolfo

Fecha:

lunes, 18 de abril de 2022

Packet Tracer: configuración de NAT estática

Objetivos

Parte 1: probar el acceso sin NAT

Parte 2: configurar NAT estática

Parte 3: probar el acceso con NAT

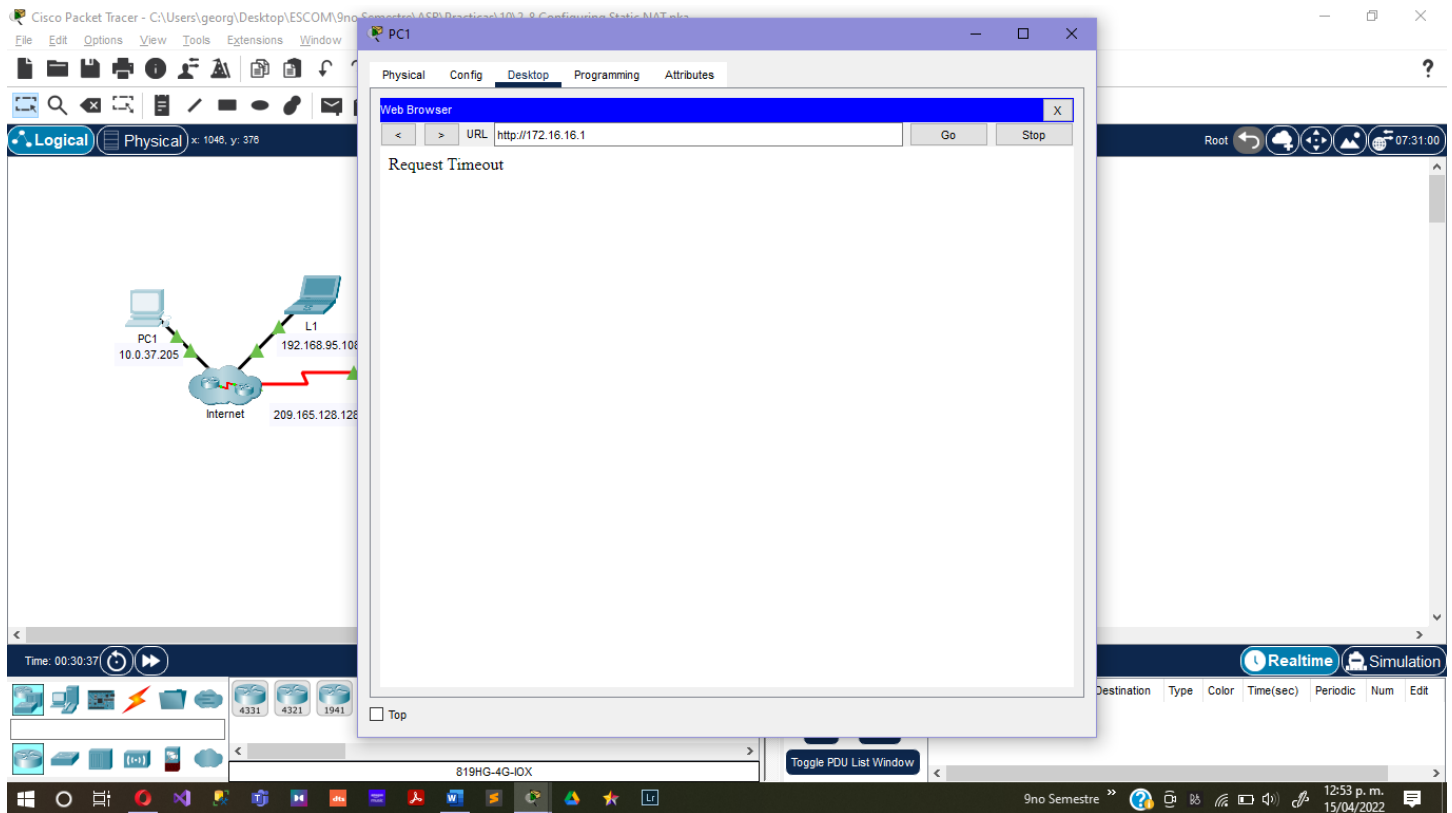
Situación

En las redes IPv4 configuradas, los clientes y los servidores utilizan direcciones privadas. Para que los paquetes con direcciones privadas puedan transmitirse por Internet, deben traducirse en direcciones públicas. Los servidores a los que se puede acceder desde fuera de la organización generalmente tienen asignadas una dirección IP estática pública y una privada. En esta actividad, deberá configurar NAT estática de modo que los dispositivos externos puedan acceder al servidor interno en su dirección pública.

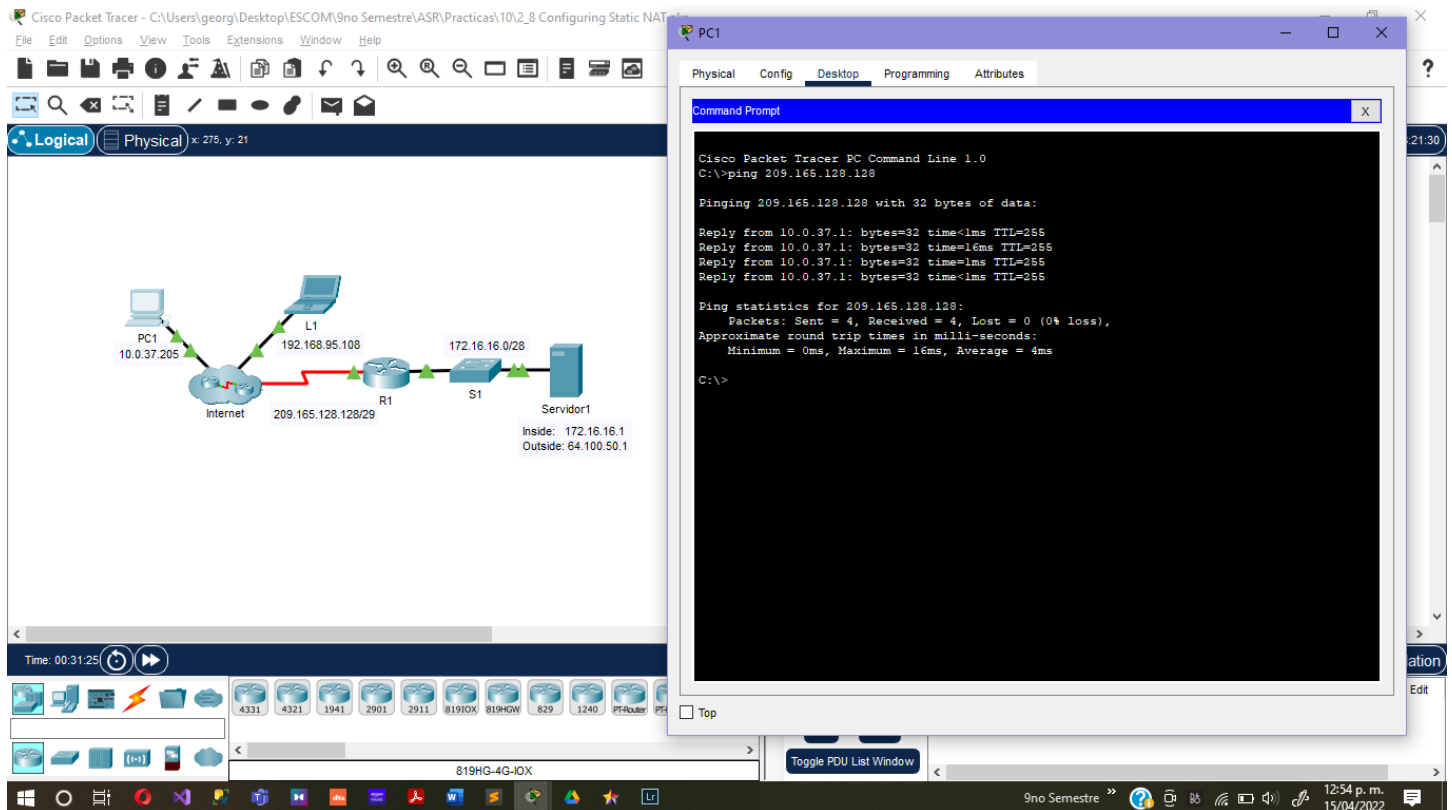
Parte 1: probar el acceso sin NAT

Paso 1: intentar conectarse al Servidor1 mediante Simulation Mode (Modo de simulación).

- a. Desde la **PC1** o la **L1**, intente conectarse a la página web de **Server1** en 172.16.16.1. Utilice el navegador web para navegar el **Servidor1** en 172.16.16.1. Los intentos deberían fallar.

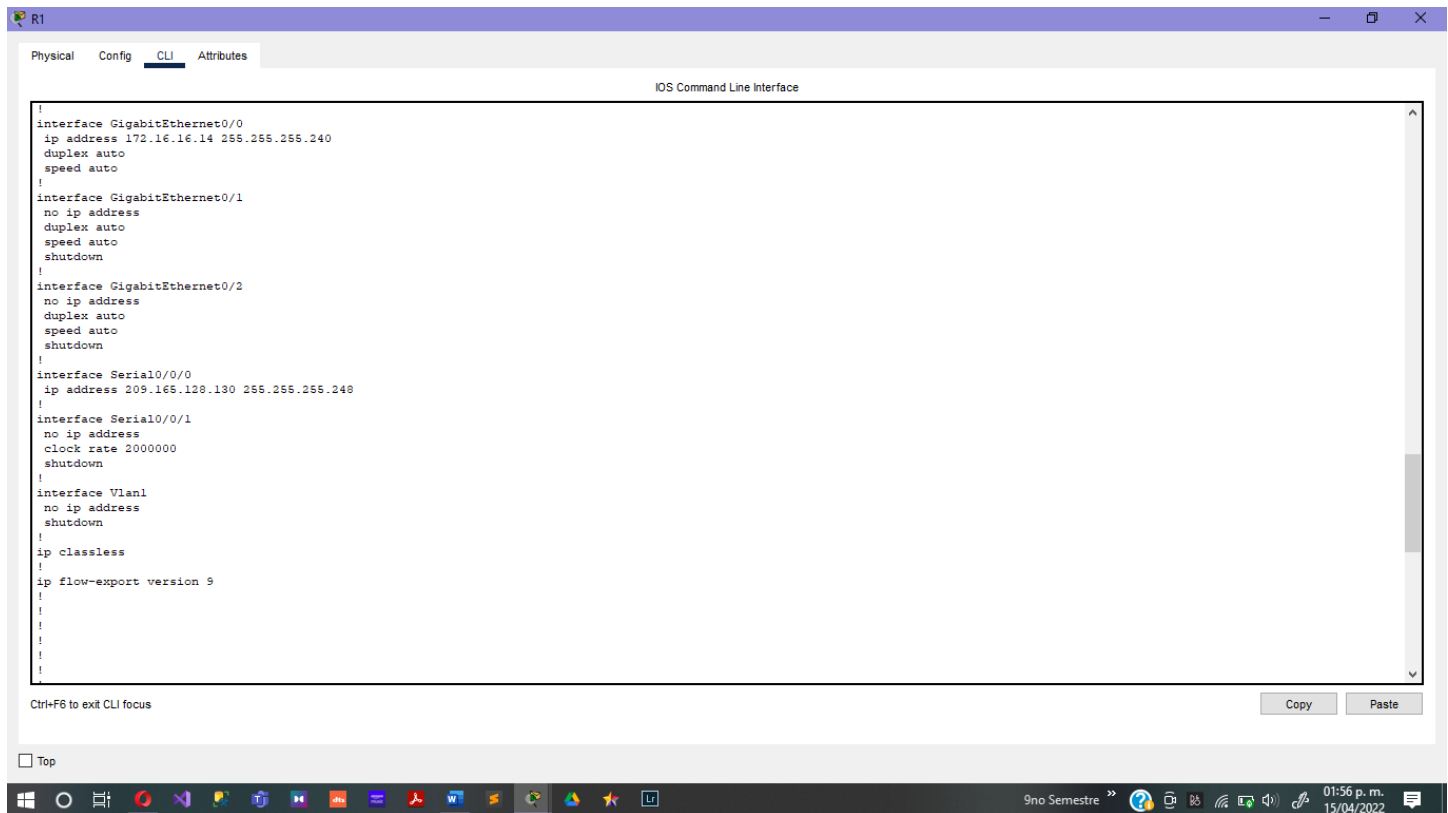


- b. Desde la **PC1**, emita un comando ping a la interfaz S0/0/0 de **R1**. El ping debe ser correcto.



Paso 2: ver la tabla de routing del R1 y la configuración en ejecución.

- a. Observe la configuración en ejecución de R1. Observe que no hay comandos que se refieran a NAT.

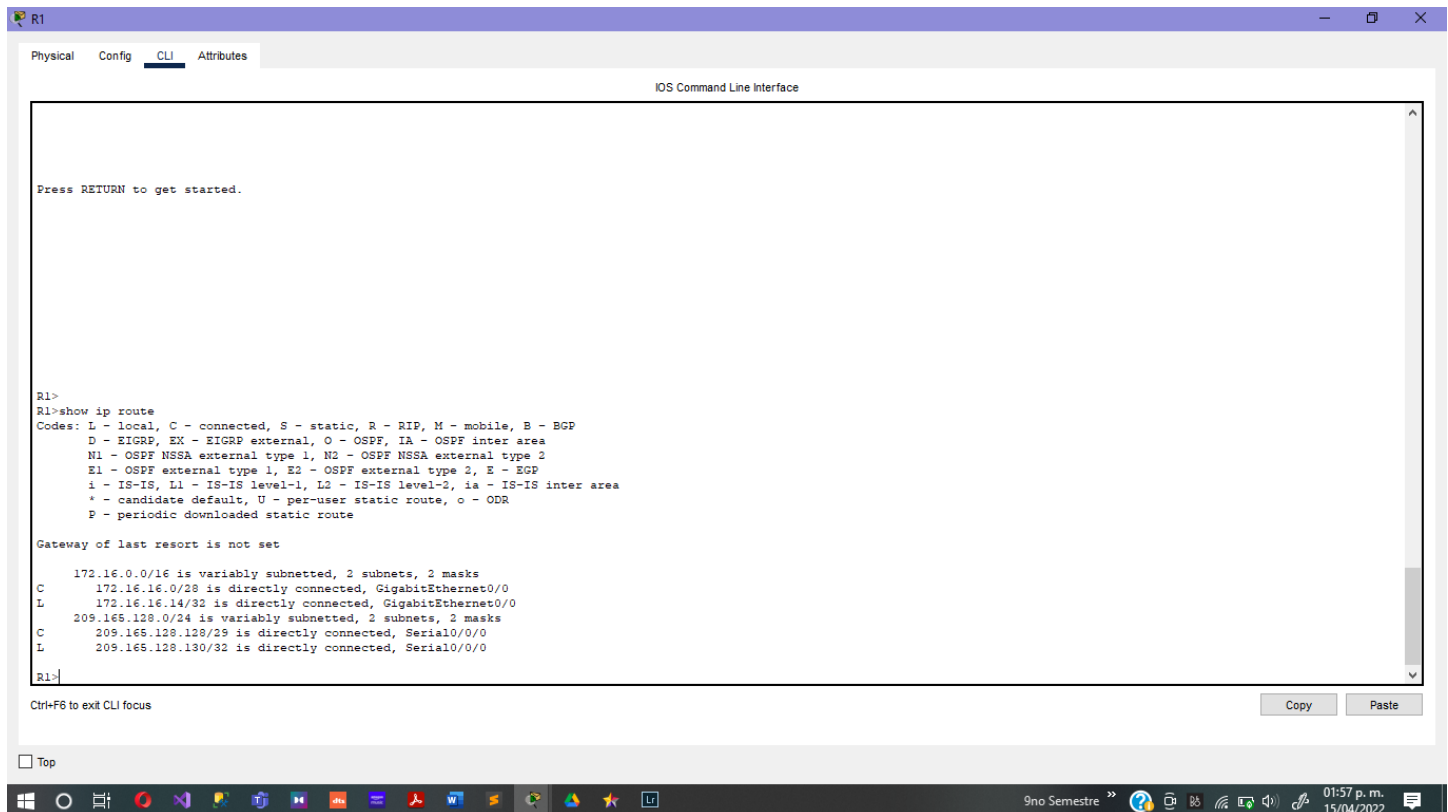


The screenshot shows the 'R1' configuration window with the 'CLI' tab selected. The 'IOS Command Line Interface' displays the running configuration. The configuration includes interfaces GigabitEthernet0/0, GigabitEthernet0/1, GigabitEthernet0/2, Serial0/0/0, Serial0/0/1, and Vlan1. It also shows the 'ip classless' command and 'ip flow-export version 9'. The configuration is as follows:

```
!
interface GigabitEthernet0/0
ip address 172.16.16.14 255.255.255.240
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 209.165.128.130 255.255.255.248
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
```

At the bottom of the CLI window, there is a 'Top' button and a 'Copy' button. The taskbar at the bottom shows the Windows taskbar with various icons and the system clock indicating 01:56 p.m. on 15/04/2022.

- b. Verifique que la tabla de routing no tenga entradas que se refieran a las direcciones IP utilizadas por la PC1 y la L1.



The screenshot shows the 'R1' configuration window with the 'CLI' tab selected. The 'IOS Command Line Interface' displays the output of the 'show ip route' command. The output shows the routing table, including the local interface addresses and the connected routes. The output is as follows:

```
Press RETURN to get started.

R1>
R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.16.0/28 is directly connected, GigabitEthernet0/0
L       172.16.16.14/32 is directly connected, GigabitEthernet0/0
C       209.165.128.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.128.128/29 is directly connected, Serial0/0/0
L       209.165.128.130/32 is directly connected, Serial0/0/0

R1>
```

At the bottom of the CLI window, there is a 'Top' button and a 'Copy' button. The taskbar at the bottom shows the Windows taskbar with various icons and the system clock indicating 01:57 p.m. on 15/04/2022.

- c. Verifique que el R1 no utilice NAT.

R1# show ip nat translations

The screenshot shows a Cisco IOS Command Line Interface (CLI) window titled "R1". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main area displays the output of the "show ip nat translations" command. The output shows two NAT pools: "172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks" and "209.165.128.0/24 is variably subnetted, 2 subnets, 2 masks". Below these, the "C" (connected) and "L" (local) addresses are listed for each pool. The "C" addresses are "172.16.16.0/28 is directly connected, GigabitEthernet0/0" and "209.165.128.0/24 is directly connected, Serial0/0/0". The "L" addresses are "172.16.16.14/32 is directly connected, GigabitEthernet0/0" and "209.165.128.130/32 is directly connected, Serial0/0/0". The CLI prompt "R1#" is visible at the bottom left of the main area. Below the main area, there is a "Ctrl+F6 to exit CLI focus" message and "Copy" and "Paste" buttons. At the bottom of the window, there is a taskbar with various application icons and a system tray showing the date and time as "01:58 p.m. 15/04/2022".

```
R1# show ip nat translations
R1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

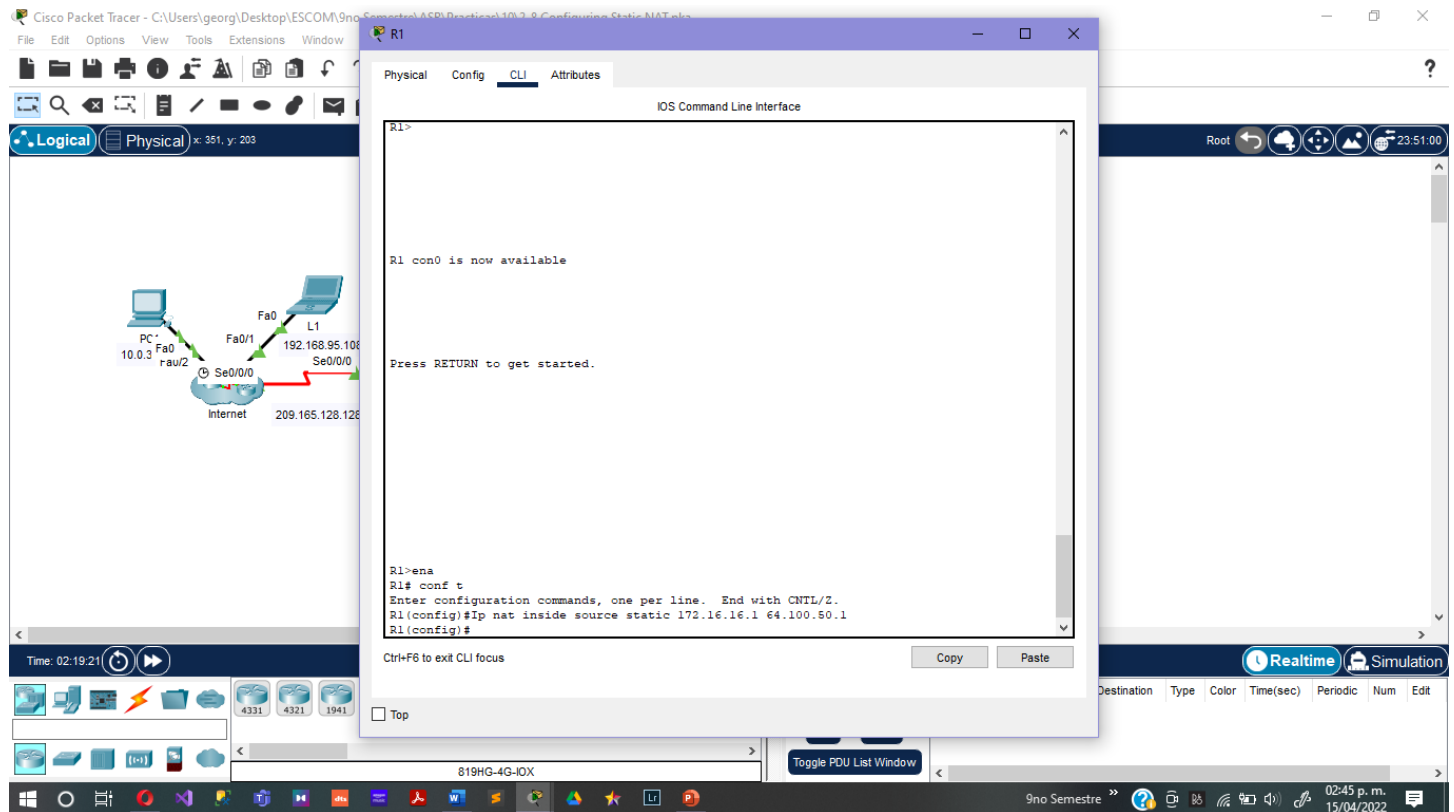
9no Semestre 01:58 p.m. 15/04/2022

Parte 2: configurar NAT estática

Paso 1: configurar instrucciones de NAT estática.

Consulte la topología. Cree una traducción de NAT estática para asignar la dirección interna del **Servidor1** a su dirección externa.

`Ip nat inside source static 172.16.16.1 64.100.50.1`



Paso 2: configurar las interfaces.

Configure las interfaces internas y externas correctas.

Interface Serial 0/0/0

`Ip nat outside`

Interface Gig 0/0

`Ip nat inside`

Cisco Packet Tracer - C:\Users\georg\Desktop\ESCOM\9no Semestre\ASPD\Practica\10\2.3-Configuring Static NAT.pka

File Edit Options View Tools Extensions Window

Logical Physical x: 351, y: 203

PC Fa0 10.0.3 rau/2 Internet 209.165.128.126

Time: 02:19:52

819HG-4G-IOX

Toggle PDU List Window

9no Semestre 02:46 p.m. 15/04/2022

R1

Physical Config CLI Attributes

IOS Command Line Interface

R1 con0 is now available

Press RETURN to get started.

R1>ena
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip nat inside source static 172.16.16.1 64.100.50.1
R1(config)#interface Serial 0/0/0
R1(config-if)#ip nat outside
R1(config-if)#interface Gig 0/0
R1(config-if)#ip nat inside
R1(config-if)#

Ctrl+F6 to exit CLI focus

Copy Paste

Realtime Simulation

Destination	Type	Color	Time(sec)	Periodic	Num	Edit
-------------	------	-------	-----------	----------	-----	------

Parte 3: probar el acceso con NAT

Paso 1: verificar la conectividad a la página web del Servidor1.

- a. Abra el símbolo del sistema en la **PC1** o la **L1**, e intente emitir el comando ping a la dirección pública de **Server1**. Los pings se deben realizar correctamente.

The screenshot shows the Cisco Packet Tracer interface. On the left, a network diagram is visible with the following components and connections:

- PC1** (10.0.3) connected to **Internet** (10.0.0/24) via Fa0/20.
- Internet** connected to **L1** (192.168.95.108) via Fa0/1.
- L1** connected to **R1** (209.165.128.29) via Se0/0/0.
- R1** connected to **S1** (172.16.16.1) via Gig0/0.
- S1** connected to **Server1** (172.16.16.1) via Fa0/1.
- Server1** has an inside IP of 172.16.16.1 and an outside IP of 64.100.50.1.

On the right, the **PC1** window is open, showing the **Command Prompt** with the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 209.165.128.128

Pinging 209.165.128.128 with 32 bytes of data:

Reply from 10.0.37.1: bytes=32 time<1ms TTL=255
Reply from 10.0.37.1: bytes=32 time=16ms TTL=255
Reply from 10.0.37.1: bytes=32 time<1ms TTL=255
Reply from 10.0.37.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.128.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 4ms

C:\>ping 64.100.50.1

Pinging 64.100.50.1 with 32 bytes of data:

Request timed out.
Reply from 64.100.50.1: bytes=32 time=12ms TTL=126
Reply from 64.100.50.1: bytes=32 time=1ms TTL=126
Reply from 64.100.50.1: bytes=32 time=10ms TTL=126

Ping statistics for 64.100.50.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 7ms

C:\>
```

- b. Verifique que tanto la **PC1** como la **L1** ahora puedan acceder a la página web de **Server1**.

The screenshot shows the Cisco Packet Tracer interface with the same network diagram as above. On the right, the **PC1** window is open, showing the **Web Browser** with the following content:

```
URL: http://64.100.50.1
Go Stop

Server1

Welcome to Server1!
```


R1

Physical Config CLI Attributes

IOS Command Line Interface

```
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source static 172.16.16.1 64.100.50.1
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end

R1#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 64.100.50.1:80      172.16.16.1:80    209.165.128.129:1025 209.165.128.129:1025
tcp 64.100.50.1:80      172.16.16.1:80    209.165.128.129:1026 209.165.128.129:1026
--- 64.100.50.1         172.16.16.1       ---                ---

R1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

9no Semestre 02:49 p.m. 15/04/2022

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
!
ip nat inside source static 172.16.16.1 64.100.50.1
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end

R1#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 64.100.50.1:80      172.16.16.1:80    209.165.128.129:1025 209.165.128.129:1025
tcp 64.100.50.1:80      172.16.16.1:80    209.165.128.129:1026 209.165.128.129:1026
--- 64.100.50.1         172.16.16.1       ---                ---

R1#show ip nat statistics
Total translations: 3 (1 static, 2 dynamic, 2 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: GigabitEthernet0/0
Hits: 17 Misses: 6
Expired translations: 4
Dynamic mappings:
R1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

9no Semestre 02:50 p.m. 15/04/2022

Cisco Packet Tracer - C:\Users\georg\Desktop\ESCOM\9no Semestre\ASR\Practicas\10\2_8 Configuring Static NAT.pka

FileEditOptionsViewToolsExtensionsWindowHelp

Activity Results

Time Elapsed: 02:29:18

Congratulations Guest! You completed the activity.

Overall Feedback

Assessment Items

Connectivity Tests

Felicitaciones. Completó correctamente la actividad de configuración de NAT estática de Packet Tracer.

Close

Windows taskbar icons: Start, Task View, File Explorer, Microsoft Edge, Visual Studio Code, Google Chrome, Word, PowerPoint, Teams, OneDrive, Outlook, etc.

9no Semestre >> ? [Icons] [Icons] [Icons] [Icons] [Icons] 02:51 p. m. 15/04/2022

Conclusiones:

Arévalo Andrade Miguel Ángel:

En esta práctica observamos el comportamiento de las NAT's que nos proporciona cierto grado de privacidad, aunque con estas no podemos ahorrar direcciones ip, aún así siguen siendo muy útiles en el campo laboral, por lo que es muy importante entender el comportamiento de estas.

Castro Cruces Jorge Eduardo:

Se lograron los objetivos de la práctica:

- Parte 1: probar el acceso sin NAT
- Parte 2: configurar NAT estática
- Parte 3: probar el acceso con NAT

López Mares Irene Elizabeth:

En esta práctica pudimos observar mejor el comportamiento de las NATs ya que permiten que las comunicaciones se inicien desde la red interna o desde una red externa, como por ejemplo Internet. Además son útiles si dentro de la red interna hay un sistema al que desea permitir el acceso de usuarios públicos. En este caso, debe crear una regla de NAT que correlacione la dirección real del sistema con una dirección pública. La dirección pública pasa a ser información externa. Con ello se garantiza que la información interna permanezca fuera del alcance de alguien cuyas intenciones pudieran ser atacar los sistemas.

Pedroza García Rodolfo:

En esta práctica pusimos en práctica la teoría vista en clase sobre las NAT's, implementando NAT's estáticas, las cuales son muy útiles ya que con estas podemos obtener cierto grado de privacidad ya que con una regla NAT podemos ocultar una ip privada con una pública con la cual los usuarios pueden acceder a los servicios.