



Instituto Politécnico Nacional



Escuela Superior de Cómputo

Práctica 2_10: Escalamiento de redes con 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

Actividad 7.2.8:

Escalabilidad de redes con NAT

NOTA PARA EL USUARIO: Si bien puede completar esta actividad sin instrucciones impresas, se ofrece una versión en PDF en la sección de texto de la misma página desde la que inició esta actividad.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
R3	Fa0/1	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252
Servidor Web interno	NIC	Local: 192.168.20.254	255.255.255.252
	NIC	Global: 209.165.202.131	255.255.255.252
PC1	NIC	192.168.10.10	255.255.255.0
PC3	NIC	192.168.30.10	255.255.255.0
Host externo	NIC	209.165.201.14	255.255.255.240
Servidor Web público	NIC	209.265.201.30	255.255.255.240

Objetivos de aprendizaje

- Configurar una ACL que permita NAT
- Configurar la NAT estática
- Configurar NAT dinámica con sobrecarga
- Configurar el router del ISP con la ruta estática
- Probar la conectividad

Introducción

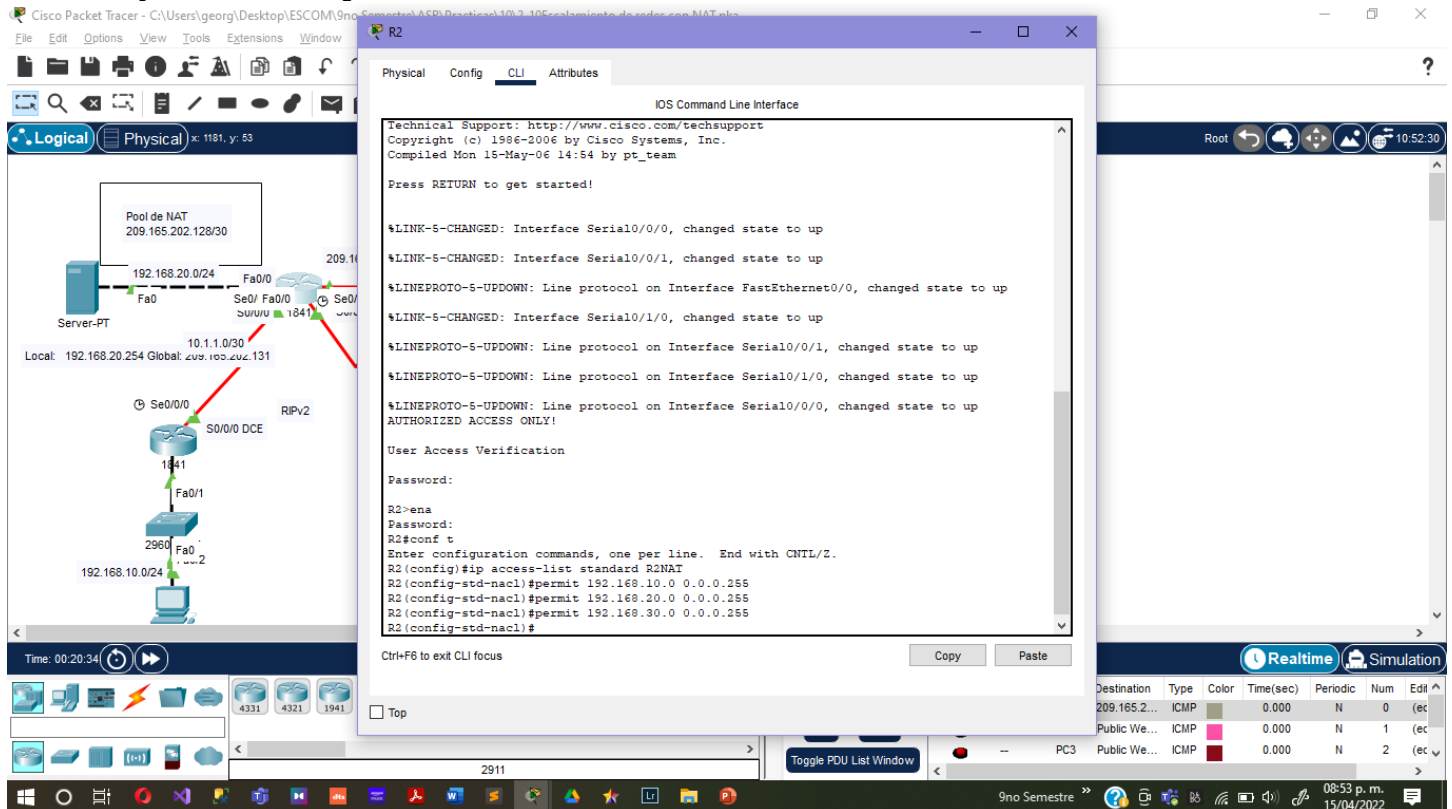
La NAT traduce las direcciones internas privadas no enrutables en direcciones públicas enrutables. NAT tiene el beneficio adicional de proporcionar a una red cierto grado de privacidad y seguridad, ya que oculta las direcciones IP internas de las redes externas. En esta actividad, se configurará NAT estática y dinámica.

Tarea 1: Configurar una ACL para permitir NAT

Paso 1. Crear una ACL estándar y nombrada.

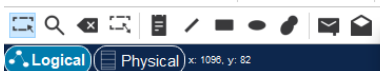
Para definir las direcciones internas que se traducen a direcciones públicas en el proceso NAT, cree una ACL estándar nombrada, llamada R2NAT. Esta lista se utiliza en los siguientes pasos de configuración de NAT.

```
R2(config)#ip access-list standard R2NAT
R2(config-std-nacl)# permit 192.168.10.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.30.0 0.0.0.255
```



Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 11%. De no ser así, haga clic en **Verificar resultados** para ver qué componentes necesarios aún no se han completado.



PT Activity: 02:44:14

Actividad 7.2.8: Escalabilidad de redes con NAT

NOTA PARA EL USUARIO: Si bien puede completar esta actividad sin instrucciones impresas, se ofrece una versión en PDF en la sección de texto de la misma página desde la que inició esta actividad.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/1	192.168.30.1	255.255.255.0

Time Elapsed: 02:44:14

Completion: 11%*

☐ Top☐ Dock

Check Results

Back

1/1

Next

Time: 00:20:50

Realtime

Simulation



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
●	—	Outsi...	209.165.2...	ICMP		0.000	N	0	(ec
●	—	PC1	Public We...	ICMP		0.000	N	1	(ec
●	—	PC3	Public We...	ICMP		0.000	N	2	(ec



9no Semestre 08:53 p. m. 15/04/2022

Tarea 2: Configurar NAT estática

Paso 1. Configurar NAT estática para un servidor Web interno.

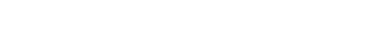
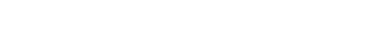
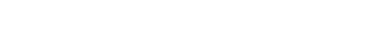
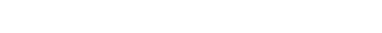
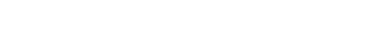
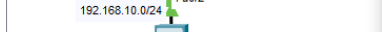
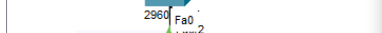
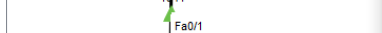
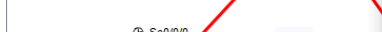
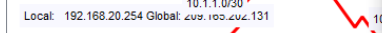
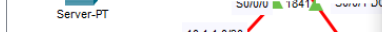
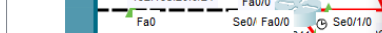
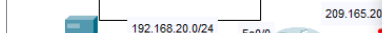
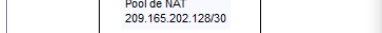
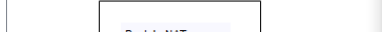
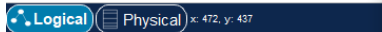
El servidor Web interno tiene que tener una dirección IP pública que nunca cambie para que se pueda acceder a él desde afuera de la red. La configuración de una dirección NAT estática permite la configuración del servidor Web con una dirección interna privada. Luego, el proceso NAT asigna paquetes mediante la dirección pública del servidor a la dirección privada.

```
R2 (config)#ip nat inside source static 192.168.20.254 209.165.202.131
```

The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a central router R2 connected to two edge routers, R1 and R3. R1 is connected to a Server-PT (192.168.20.254) and a pool of NAT (209.165.202.128/30). R3 is connected to a pool of NAT (209.165.202.224/27). The configuration window for R2 shows the following commands: R2>ena, Password: R2#conf t, R2 (config)#ip access-list standard R2NAT, R2 (config-std-nacl)#permit 192.168.10.0 0.0.0.255, R2 (config-std-nacl)#permit 192.168.20.0 0.0.0.255, R2 (config-std-nacl)#exit, R2 (config)#ip nat inside source static 192.168.20.254 209.165.202.131, R2 (config)#. The status window shows the configuration is successful.

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 22%. De no ser así, haga clic en **Verificar resultados** para ver qué componentes necesarios aún no se han completado.



PT Activity: 02:45:59

Actividad 7.2.8: Escalabilidad de redes con NAT

NOTA PARA EL USUARIO: Si bien puede completar esta actividad sin instrucciones impresas, se ofrece una versión en PDF en la sección de texto de la misma página desde la que inició esta actividad.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/1	192.168.30.1	255.255.255.0

Time Elapsed: 02:45:59

Completion: 22%*

☐ Top☐ Dock

Check Results

Back

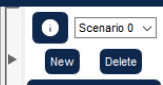
1/1

Next

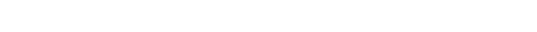
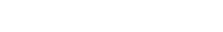
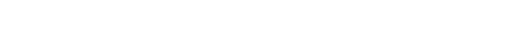
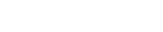
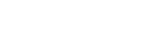
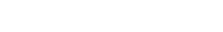
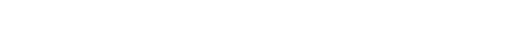
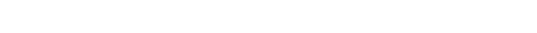
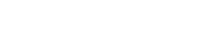
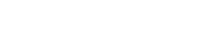
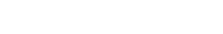
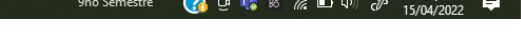
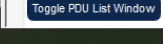
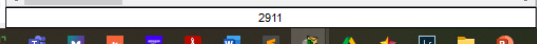
Time: 00:22:28

Realtime

Simulation



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
●	---	Outsi...	209.165.2...	ICMP		0.000	N	0	(ec
●	---	PC1	Public We...	ICMP		0.000	N	1	(ec
●	---	PC3	Public We...	ICMP		0.000	N	2	(ec



Tarea 3: Configurar NAT dinámica con sobrecarga

Además de la dirección IP pública asignada al servidor Web interno, el ISP ha asignado tres direcciones públicas para que las use. Estas direcciones se asignan a todos los demás hosts internos que acceden a Internet.

Para permitir que más de tres hosts internos accedan a Internet al mismo tiempo, configure la NAT con sobrecarga para incorporar los hosts adicionales. NAT con sobrecarga, llamada también Traducción de la dirección del puerto (PAT), utiliza números de puerto para distinguir paquetes de diferentes hosts que se asignan a la misma dirección IP pública.

Paso 1. Definir el conjunto de direcciones y configurar NAT dinámica.

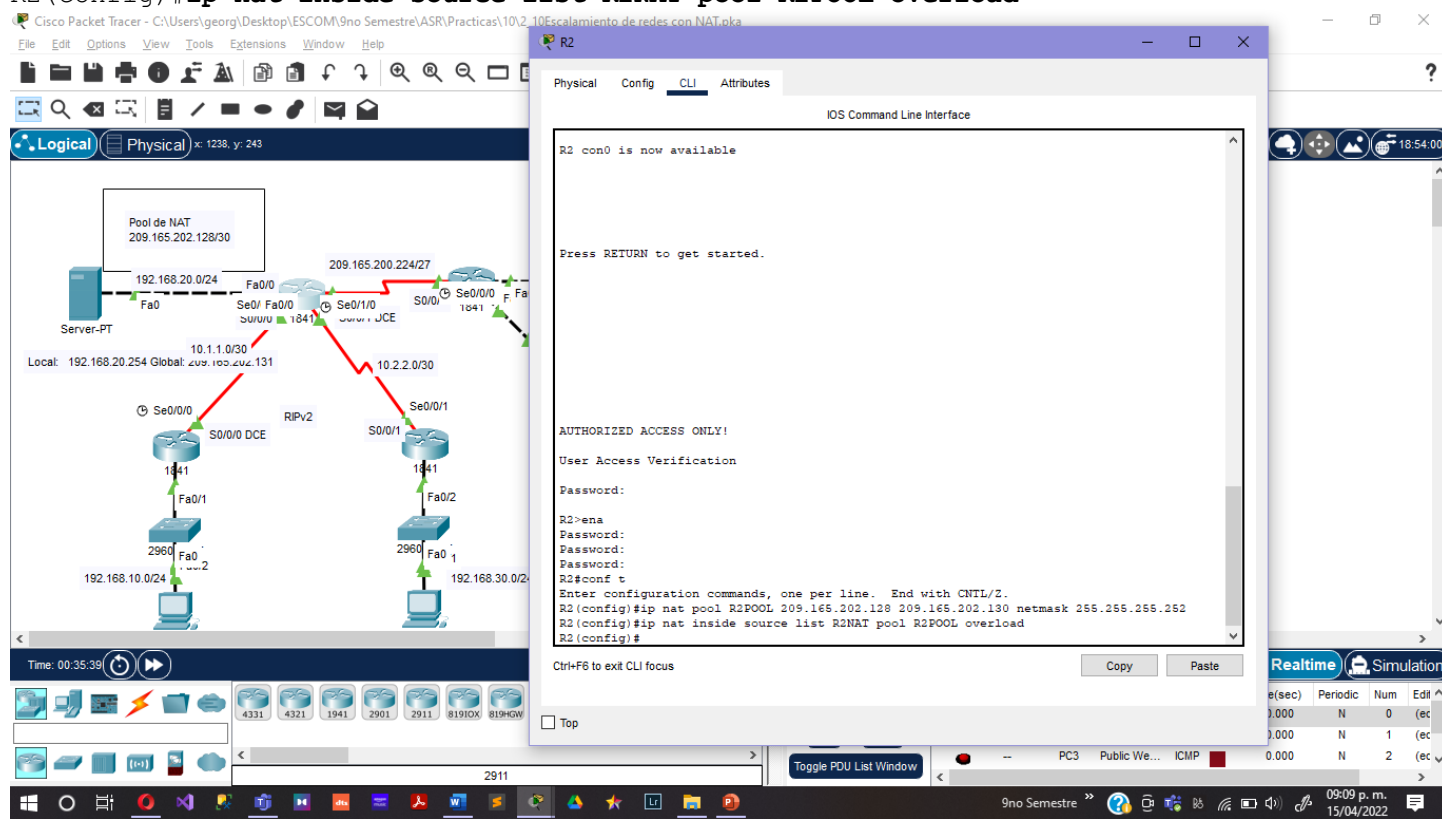
Ingresa los siguientes comandos para configurar el conjunto de direcciones públicas que se asignan en forma dinámica a los hosts internos.

El primer comando define el conjunto de tres direcciones públicas que se asignan a direcciones internas.

El segundo comando indica al proceso NAT que asigna las direcciones en el pool a las direcciones definidas en la lista de acceso que se creó en la Tarea 1.

```
R2(config)#ip nat pool R2POOL 209.165.202.128 209.165.202.130 netmask 255.255.255.252
```

```
R2(config)#ip nat inside source list R2NAT pool R2POOL overload
```



The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a Server-PT connected to a switch (S1) and a router (R1). R1 is connected to another switch (S2) and a router (R2). R2 is connected to the Internet. The diagram includes IP addresses for various interfaces and a NAT pool configuration. On the right, the CLI window for R2 is open, showing the configuration commands being entered:

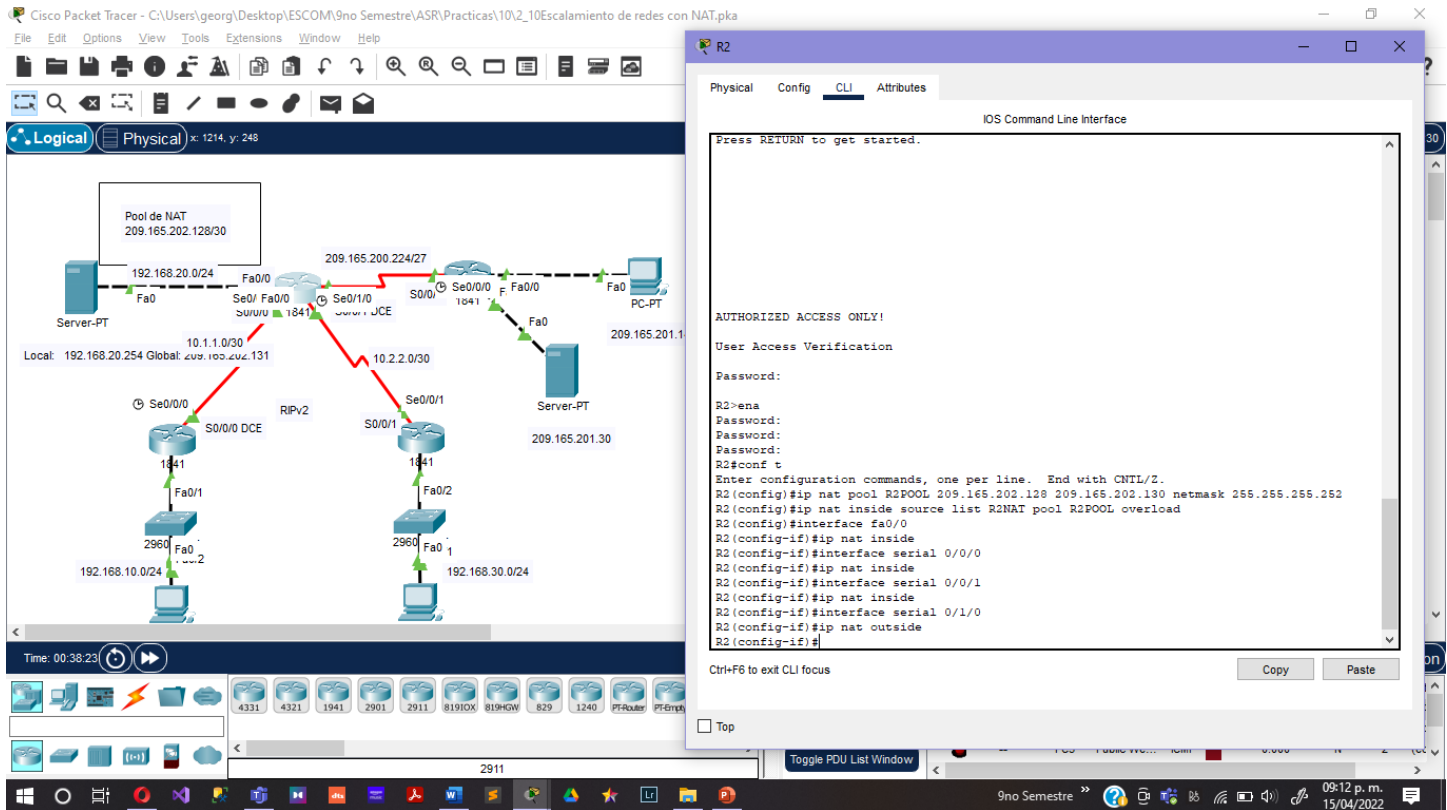
```
R2 con0 is now available

Press RETURN to get started.

AUTHORIZED ACCESS ONLY!
User Access Verification
Password:
R2>ena
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip nat pool R2POOL 209.165.202.128 209.165.202.130 netmask 255.255.255.252
R2(config)#ip nat inside source list R2NAT pool R2POOL overload
R2(config)#
```

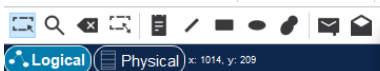
Paso 2. Configurar las interfaces en R2 para aplicar NAT.

En el modo configuración de interfaz en R2, configure cada una de las interfaces mediante el comando **ip nat {inside | outside}**. Debido a que las direcciones internas están en redes conectadas a las interfaces Fa0/0, Serial 0/0/0 y Serial0/0/1, use el comando **ip nat inside** al configurar estas interfaces. Internet está conectada a Serial0/1/0; por lo tanto, utilice el comando **ip nat outside** en esta interfaz.



Paso 3. Verificar los resultados.

Su porcentaje de finalización debe ser del 89%. De no ser así, haga clic en **Verificar resultados** para ver qué componentes necesarios aún no se han completado.



PT Activity: 03:03:08

Actividad 7.2.8: Escalabilidad de redes con NAT

NOTA PARA EL USUARIO: Si bien puede completar esta actividad sin instrucciones impresas, se ofrece una versión en PDF en la sección de texto de la misma página desde la que inició esta actividad.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/1	192.168.30.1	255.255.255.0

Time Elapsed: 03:03:08

Completion: 88%*

☐ Top ☐ Dock

1/1

Time: 00:38:36

☒ Realtime☐ Simulation

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
●	—	Outsi...	209.165.2...	ICMP		0.000	N	0	(ec
●	—	PC1	Public We...	ICMP		0.000	N	1	(ec
●	—	PC3	Public We...	ICMP		0.000	N	2	(ec



9no Semestre 09:12 p. m. 15/04/2022

Tarea 4: Configurar ISP con una ruta estática

Paso 1. Configurar ISP con una ruta estática a R2.

ISP requiere una ruta estática a las direcciones públicas de R2. Use el siguiente comando para configurar esta ruta.

```
ISP(config)#ip route 209.165.202.128 255.255.255.224 serial0/0/0
```

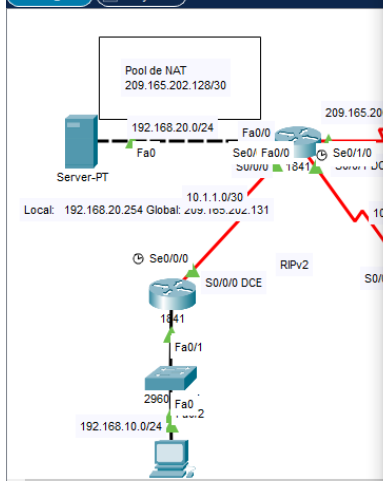
The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a 'Server-PT' connected to a router labeled 'ISP' via its 'Fa0/0' interface. The ISP is connected to a serial interface 'Se0/0/0', which is connected to another router 'R2' via its 'Se0/0/0' interface. R2 is connected to a PC. The ISP is configured with a static route to the public IP address 209.165.202.128/24 via its serial interface. The CLI window shows the configuration commands: 'enable', 'configure terminal', and 'ip route 209.165.202.128 255.255.255.224 serial0/0/0'. The status bar at the bottom shows the simulation is running in Realtime mode.

Paso 2. Verificar los resultados.

Su porcentaje de finalización debe ser del 100%. De no ser así, haga clic en **Verificar resultados** para ver qué componentes necesarios aún no se han completado.



Logical Physical x: 1096, y: 161



PT Activity: 03:04:52

Actividad 7.2.8: Escalabilidad de redes con NAT

NOTA PARA EL USUARIO: Si bien puede completar esta actividad sin instrucciones impresas, se ofrece una versión en PDF en la sección de texto de la misma página desde la que inició esta actividad.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/1	192.168.30.1	255.255.255.0

Time Elapsed: 03:04:52

Completion: 100%*

☐ Top☐ Dock

Check Results

Back

1/1

Next

Time: 00:40:13

Realtime

Simulation



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
---	---	Outsi...	209.165.2...	ICMP		0.000	N	0	(ec
---	---	PC1	Public We...	ICMP		0.000	N	1	(ec
---	---	PC3	Public We...	ICMP		0.000	N	2	(ec

Tarea 5: Probar la conectividad

Ahora debe poder hacer ping desde cualquier host interno a un host externo o un servidor Web público.

The screenshot displays the Cisco Packet Tracer interface with a network topology for NAT. The network includes a Server-PT, two routers (R1, R2), and two PCs (PC1, PC2). A NAT pool is configured on R1. The Event List panel shows a sequence of ICMP events from PC1 to R1, R2, and the Outside Host.

Vis.	Time(sec)	Last Device	At Device	Type
0.000	--	PC1		ICMP
0.001		PC1	S1	ICMP
0.002		S1	R1	ICMP
0.003		R1	R2	ICMP
0.004		R2	ISP	ICMP
0.005		ISP	Outside Host	ICMP
0.006		Outside Host	ISP	ICMP
0.007		ISP	R2	ICMP
0.008		R2	R1	ICMP
0.009		R1	S1	ICMP

Para comprobar los efectos de NAT en un paquete específico, ingrese al modo Simulación y observe el paquete que se origina en la PC1.

Haga clic en el cuadro de color con información asociado con ese paquete cuando pasa de R1 a R2. Al hacer clic en **Detalles de la PDU entrante**, se puede observar que la dirección de origen es 192.168.10.10. Al hacer clic en **Detalles de la PDU saliente**, se puede observar que la dirección de origen se tradujo a una dirección 209.165.x.x.

Cisco Packet Tracer - C:\Users\georg\Desktop\ESCOM\9no Semestre\ASR\Practicas\10_2_10Escalaiento de redes con NAT.pka

File Edit Options View Tools Extensions Window Help

Logical Physical x: 697, y: 425

Pool de NAT
209.165.202.128/30

Server-PT
192.168.20.0/24
Fa0

Local: 192.168.20.254 Global: 209.165.202.131

10.1.1.0/30
Se0/0/0
S0/0/0 DCE

10.2.2.0/30
Se0/0/1
S0/0/1

RIPV2

2960
Fa0/1
Fa0/2

192.168.10.0/24

Time: 00:53:37.345 PLAY CONTROLS

PDU Information at Device: R2

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

HDLCL

0 8 16 24 Bits

FLG: 0x7E ADR: 0x8f CONTROL: 0x0000

DATA (VARIABLE LENGTH)

FCS: 0x0000 FLG: 0x7E

IP

0 4 8 16 20 24 Bits

VER: 4 IHL: 5 DSCP: 0x00 TL: 28

ID: 0x0002 FLA: 0x0000 FRAG OFFSET: 0x000

TTL: 254 PRO: 0x01 CHKSUM

SRC IP: 192.168.10.10

DST IP: 209.165.201.14

DATA (VARIABLE LENGTH)

ICMP

Device Type

1 Device ICMP

2 Device ICMP

3 Device ICMP

4 Device ICMP

5 Device ICMP

6 Device ICMP

7 Device ICMP

8 Device ICMP

9 Device ICMP

10 Device ICMP

11 Device ICMP

12 Device ICMP

13 Device ICMP

14 Device ICMP

15 Device ICMP

16 Device ICMP

17 Device ICMP

18 Device ICMP

19 Device ICMP

20 Device ICMP

21 Device ICMP

22 Device ICMP

23 Device ICMP

24 Device ICMP

25 Device ICMP

26 Device ICMP

27 Device ICMP

28 Device ICMP

29 Device ICMP

30 Device ICMP

31 Device ICMP

Captured to: 738.567 s

Event List Realtime Simulation

Scenario 0

New Delete

Toggle PDU List Window

Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit

Successful PC1 Outside Host ICMP 0.000 N 0 (edt)

9no Semestre 09:20 p. m. 15/04/2022

Cisco Packet Tracer - C:\Users\georg\Desktop\ESCOM\9no Semestre\ASR\Practicas\10_2_10Escalaiento de redes con NAT.pka

File Edit Options View Tools Extensions Window Help

Logical Physical x: 697, y: 425

Pool de NAT
209.165.202.128/30

Server-PT
192.168.20.0/24
Fa0

Local: 192.168.20.254 Global: 209.165.202.131

10.1.1.0/30
Se0/0/0
S0/0/0 DCE

10.2.2.0/30
Se0/0/1
S0/0/1

RIPV2

2960
Fa0/1
Fa0/2

192.168.10.0/24

Time: 00:53:37.345 PLAY CONTROLS

PDU Information at Device: R2

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

HDLCL

0 8 16 24 Bits

FLG: 0x7E ADR: 0x8f CONTROL: 0x0000

DATA (VARIABLE LENGTH)

FCS: 0x0000 FLG: 0x7E

IP

0 4 8 16 20 24 Bits

VER: 4 IHL: 5 DSCP: 0x00 TL: 28

ID: 0x0002 FLA: 0x0000 FRAG OFFSET: 0x000

TTL: 253 PRO: 0x01 CHKSUM

SRC IP: 209.165.202.129

DST IP: 209.165.201.14

DATA (VARIABLE LENGTH)

ICMP

Device Type

1 Device ICMP

2 Device ICMP

3 Device ICMP

4 Device ICMP

5 Device ICMP

6 Device ICMP

7 Device ICMP

8 Device ICMP

9 Device ICMP

10 Device ICMP

11 Device ICMP

12 Device ICMP

13 Device ICMP

14 Device ICMP

15 Device ICMP

16 Device ICMP

17 Device ICMP

18 Device ICMP

19 Device ICMP

20 Device ICMP

21 Device ICMP

22 Device ICMP

23 Device ICMP

24 Device ICMP

25 Device ICMP

26 Device ICMP

27 Device ICMP

28 Device ICMP

29 Device ICMP

30 Device ICMP

31 Device ICMP

Captured to: 738.567 s

Event List Realtime Simulation

Scenario 0

New Delete

Toggle PDU List Window

Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit

Successful PC1 Outside Host ICMP 0.000 N 0 (edt)

9no Semestre 09:20 p. m. 15/04/2022

Conclusiones:

Arévalo Andrade Miguel Ángel:

Esta práctica nos ayudó a entender el funcionamiento del escalamiento NAT, lo cual es muy importante para el ambiente laboral ya que nos proporciona características que son muy útiles para las empresas.

Castro Cruces Jorge Eduardo:

Se lograron los objetivos de la práctica:

- Configurar una ACL que permita NAT
- Configurar la NAT estática
- Configurar NAT dinámica con sobrecarga
- Configurar el router del ISP con la ruta estática
- Probar la conectividad

López Mares Irene Elizabeth:

Esta práctica es muy importante ya que nos muestra los pasos para realizar un escalamiento con NAT, lo cual es algo básico que debemos aprender ya que en el ambiente laboral las empresas crecen constantemente y con ello también es necesario que las redes lo hagan y nosotros como ingenieros en sistemas debemos estar preparados para este tipo de escenarios.

Pedroza García Rodolfo:

En esta práctica aprendimos a implementar un escalamiento NAT, lo cual es muy importante ya que nos proporciona cierto grado de privacidad, además de que podemos ahorrar direcciones IP. Este tipo de conocimiento es muy importante para el ambiente laboral.