INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Administración de Servicios en Red

3.2 Configuración de NAT dinámica y estática

PROFESORA: Henestrosa Carrasco Leticia

Equipo 3

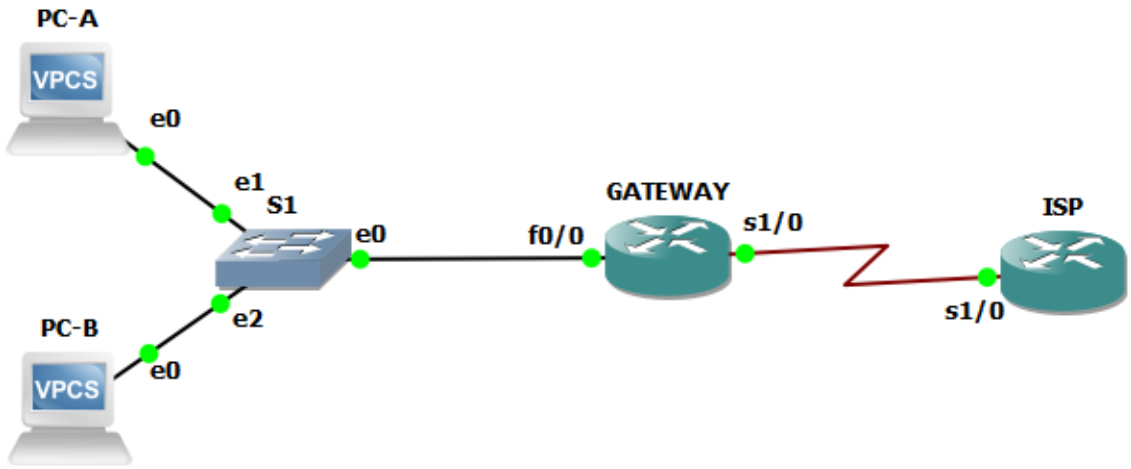
- Cruz Chávez Alan Francisco
- Gómez Salas Hugo Santiago
- Mendoza Rodríguez Israel
- Ramírez Galindo Karina

GRUPO: 4CV13

Contenido

Desarrollo

Topología



Tablas de direccionamiento

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	F0/0	192.168.1.1	255.255.255.0	N/D
	S1/0	209.165.201.18	255.255.255.252	N/D
ISP	S1/0 (DCE)	209.165.201.17	255.255.255.252	N/D
	Lo0	192.31.7.1	255.255.255.255	N/D
PC-A (servidor simulado)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Objetivos

- **Parte 1: Armar la red y verificar la conectividad**
- **Parte 2: Configurar y verificar la NAT estática**
- **Parte 3: Configurar y verificar la NAT dinámica**

Aspectos Básicos / Situación

La traducción de direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada.

En esta práctica de laboratorio, un ISP asignó a una empresa el espacio de direcciones IP públicas 209.165.200.224/27. Esto proporciona 30 direcciones IP públicas a la empresa. Las direcciones 209.165.200.225 a 209.165.200.241 son para la asignación estática, y las direcciones 209.165.200.242 a 209.165.200.254 son para la asignación dinámica. Del ISP al router de gateway se usa una ruta estática, y del gateway al router ISP se usa una ruta predeterminada. La conexión del ISP a Internet se simula mediante una dirección de loopback en el router ISP.

Configuración

Parte 1. Armar la red y verificar la conectividad

En la parte 1, establecerá la topología de la red en el emulador que refiera su instructor y configurará los parámetros básicos, como las direcciones IP de interfaz, el routing estático, el acceso a los dispositivos y las contraseñas.

Paso 1. Realizar en el emulador la topología como se muestra en la imagen de arriba

Conecte los dispositivos como se muestra en la topología.

Paso 2. Configurar los hosts de las PC

Configuración del GATEWAY:

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#int fa0/0
GATEWAY(config-if)#ip address 192.168.1.1 255.255.255.0
GATEWAY(config-if)#no shut
GATEWAY(config-if)#exit
GATEWAY(config)#int s1/0
GATEWAY(config-if)#ip address 209.165.201.18 255.255.255.252
GATEWAY(config-if)#no shut
GATEWAY(config-if)#end
GATEWAY#copy running-config startup-config
*Mar  1 00:00:23.263: %SYS-5-CONFIG_I: Configured from console by console
GATEWAY#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
GATEWAY#
*Mar  1 00:00:25.095: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:00:25.231: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
*Mar  1 00:00:26.291: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Mar  1 00:00:26.291: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
GATEWAY#
```

Configuración de la PC-A:

```
PC-A> ip 192.168.1.20 255.255.255.0 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.20 255.255.255.0 gateway 192.168.1.1

PC-A>
```

Configuración de la PC-B:

```
PC-B> ip 192.168.1.21 255.255.255.0 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.21 255.255.255.0 gateway 192.168.1.1

PC-B>
```

Configuración del ISP:

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#int s1/0
ISP(config-if)#ip address 209.165.201.17 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#exit
ISP(config)#int Lo0
ISP(config-if)#ip address 192.31.7.1 255.255.255.255
ISP(config-if)#end
ISP#copy running-config startup-config
Destination filename [startup-config]?
*Mar  1 00:25:54.127: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 00:25:55.055: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

*Mar  1 00:25:55.823: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
*Mar  1 00:25:56.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

Building configuration...
[OK]
ISP#
```

Paso 3. Inicializar y volver a cargar los routers y los switches según sea necesario

Paso 4. Configurar los ajustes básicos de cada router

a) Acceda al router e ingrese al modo de configuración global.
b) Copie la siguiente configuración básica y péguela en la configuración en ejecución en el router.

```
no ip domain-lookup
service password-encryption enable secret escom
banner motd #
Unauthorized access is strictly prohibited. # línea con 0
password ipn
 login
logging synchronous
line vty 0 4
password ipn
login
```

c) Configure el nombre de host como se muestra en la topología.
d) Copie la configuración en ejecución en la configuración de inicio

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#no ip domain-lookup
GATEWAY(config)#service password-encryption
GATEWAY(config)#enable secret escom
GATEWAY(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Unauthorized access is strictly prohibited. #
GATEWAY(config)#line con 0
GATEWAY(config-line)#password ipn
GATEWAY(config-line)#login
GATEWAY(config-line)#logging synchronous
GATEWAY(config-line)#line vty 0 4
GATEWAY(config-line)#password ipn
GATEWAY(config-line)#login
GATEWAY(config-line)#end
GATEWAY#copy running-config startup-config
*Mar  1 00:17:07.707: %SYS-5-CONFIG_I: Configured from console by console
GATEWAY#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
GATEWAY#
```

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#no ip domain-lookup
ISP(config)#service password-encryption
ISP(config)#enable secret escom
ISP(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Unauthorized access is strictly prohibited. #
ISP(config)#line con 0
ISP(config-line)#password ipn
ISP(config-line)# login
ISP(config-line)#logging synchronous
ISP(config-line)#line vty 0 4
ISP(config-line)#password ipn
ISP(config-line)#login
ISP(config-line)#end
ISP#copy running-config startup-config
Destination filename [startup-config]?
*Mar  1 00:19:35.731: %SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
ISP#
```

Paso 5. Crear un servidor web simulado en el ISP

a) Cree un usuario local denominado **webuser** con la contraseña cifrada **webpass.**
```
ISP(config)# username webuser privilege 15 secret webpass
```
b) Habilite el servicio del servidor HTTP en el ISP.
```
ISP(config)# ip http server
```
c) Configure el servicio HTTP para utilizar la base de datos local.
```
ISP(config)# ip http authentication local
```

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#username webuser privilege 15 secret webpass
ISP(config)#ip http server
ISP(config)#ip http authentication local
ISP(config)#end
ISP#copy running-config startup-config
*Mar  1 00:21:38.703: %SYS-5-CONFIG_I: Configured from console by console
ISP#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
```

Paso 6. Configurar el routing estático

a) Cree una ruta estática del router ISP al router Gateway usando el rango asignado de direcciones de redpúblicas 209.165.200.224/27.
```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#ip route 209.165.200.224 255.255.255.224 209.165.201.18
ISP(config)#end
ISP#copy running-config startup-config
*Mar  1 00:22:22.043: %SYS-5-CONFIG_I: Configured from console by console
ISP#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
```

b) Cree una ruta predeterminada del router Gateway al router ISP.
```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.17
GATEWAY(config)#end
GATEWAY#copy running-config startup-config
*Mar  1 00:25:46.639: %SYS-5-CONFIG_I: Configured from console by console
GATEWAY#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
GATEWAY#
```

Paso 7. Guardar la configuración en ejecución en la configuración de arranque

Paso 8. Verificar la conectividad de red

a) Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.

```
PC-A> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=255 time=15.712 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=255 time=15.299 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=255 time=15.277 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=255 time=15.202 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=255 time=15.322 ms

PC-A>
```

```
PC-B> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=255 time=15.309 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=255 time=15.271 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=255 time=15.203 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=255 time=15.399 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=255 time=15.179 ms

PC-B>
```

b) Muestre las tablas de routing en ambos routers para verificar que las rutas estáticas se encuentren en la tabla de routing y estén configuradas correctamente en ambos routers.

```
GATEWAY#show ip route
Codes: 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
       i - IS-IS, su - IS-IS summary, 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 209.165.201.17 to network 0.0.0.0

     209.165.201.0/30 is subnetted, 1 subnets
C       209.165.201.16 is directly connected, Serial1/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 209.165.201.17
GATEWAY#
```

```
ISP#show ip route
Codes: 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
       i - IS-IS, su - IS-IS summary, 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

     209.165.200.0/27 is subnetted, 1 subnets
S       209.165.200.224 [1/0] via 209.165.201.18
     209.165.201.0/30 is subnetted, 1 subnets
C       209.165.201.16 is directly connected, Serial1/0
     192.31.7.0/32 is subnetted, 1 subnets
C       192.31.7.1 is directly connected, Loopback0
ISP#
```

Parte 2. Configurar y verificar la NAT estática

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales, y estas asignaciones se mantienen constantes. La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener direcciones estáticas que sean accesibles desde Internet.

Paso 1. Configurar una asignación estática

El mapa estático se configura para indicarle al router que traduzca entre la dirección privada del servidor interno 192.168.1.20 y la dirección pública 209.165.200.225. Esto permite que los usuarios de Internet accedan a la PC-A. La PC-A simula un servidor o un dispositivo con una dirección constante a la que se puede acceder desde Internet.

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#ip nat inside source static 192.168.1.20 209.165.200.225
GATEWAY(config)#end
GATEWAY#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
GATEWAY#
*Mar  1 00:32:40.043: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 00:32:41.031: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
GATEWAY#
```

Paso 2. Especificar las interfaces

Emita los comandos **ip nat inside** e **ip nat outside** en las interfaces.

```
Gateway(config)# interface g0/1

Gateway(config-if)# ip nat inside

Gateway(config-if)# interface s0/0/1

Gateway(config-if)# ip nat outside
```

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#int fa0/0
GATEWAY(config-if)#ip nat inside
GATEWAY(config-if)#int s1/0
GATEWAY(config-if)#ip nat outside
GATEWAY(config-if)#end
GATEWAY#copy running-config startup-config
*Mar  1 00:33:50.547: %SYS-5-CONFIG_I: Configured from console by console
GATEWAY#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
GATEWAY#
```

Paso 3. Probar la configuración

a. Muestre la tabla de NAT estática mediante la emisión del comando **show ip nat translations**.

```
Gateway# show ip nat translations
```

```
GATEWAY#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
GATEWAY#
```

¿Cuál es la traducción de la dirección host local interna?
192.168.1.20 = 209.165.200.225
¿Quién asigna la dirección global interna?
El router del pool de la NAT
¿Quién asigna la dirección local interna?
El administrador de la estación de trabajo

b. En la PC-A, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija losproblemas. En el router Gateway, muestre la tabla de NAT.

```
PC-A> ping 192.31.7.1
84 bytes from 192.31.7.1 icmp_seq=1 ttl=254 time=45.123 ms
84 bytes from 192.31.7.1 icmp_seq=2 ttl=254 time=45.181 ms
84 bytes from 192.31.7.1 icmp_seq=3 ttl=254 time=45.216 ms
84 bytes from 192.31.7.1 icmp_seq=4 ttl=254 time=45.277 ms
84 bytes from 192.31.7.1 icmp_seq=5 ttl=254 time=45.215 ms
```

```
Gateway# show ip nat translations
```

```
GATEWAY#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
GATEWAY#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:6375 192.168.1.20:6375 192.31.7.1:6375  192.31.7.1:6375
icmp 209.165.200.225:6631 192.168.1.20:6631 192.31.7.1:6631  192.31.7.1:6631
icmp 209.165.200.225:6887 192.168.1.20:6887 192.31.7.1:6887  192.31.7.1:6887
icmp 209.165.200.225:7143 192.168.1.20:7143 192.31.7.1:7143  192.31.7.1:7143
icmp 209.165.200.225:7399 192.168.1.20:7399 192.31.7.1:7399  192.31.7.1:7399
--- 209.165.200.225    192.168.1.20       ---                ---
GATEWAY#
```

Cuando la PC-A envió una solicitud de ICMP (ping) a la dirección 192.31.7.1 en el ISP, se agregó a latabla una entrada de NAT en la que se indicó ICMP como protocolo.

¿Qué número de puerto se usó en este intercambio ICMP? 6775 (puede variar)

Nota: Puede ser necesario desactivar el firewall de la PC-A para que el ping se realice correctamente.

c. En la PC-A, acceda a la interfaz Lo0 del ISP mediante telnet y muestre la tabla de NAT.

```
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23 192.31.7.1:23
--- 209.165.200.225      192.168.1.20       ---               ---
```

Nota: Es posible que se haya agotado el tiempo para la NAT de la solicitud de ICMP y se haya eliminadode la tabla de NAT.

¿Qué protocolo se usó para esta traducción? TCP

¿Cuáles son los números de puerto que se usaron?

Global/local interno: 1034 (puede variar)

Global/local externo: 23

d. Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.

```
PC-A> ping 209.165.200.225
84 bytes from 209.165.200.225 icmp_seq=1 ttl=61 time=90.373 ms
84 bytes from 209.165.200.225 icmp_seq=2 ttl=61 time=90.314 ms
84 bytes from 209.165.200.225 icmp_seq=3 ttl=61 time=90.445 ms
84 bytes from 209.165.200.225 icmp_seq=4 ttl=61 time=90.165 ms
84 bytes from 209.165.200.225 icmp_seq=5 ttl=61 time=90.317 ms

PC-A>
```

e. En el router Gateway, muestre la tabla de NAT para verificar la traducción.

```
Gateway# show ip nat translations
```

```
GATEWAY#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
GATEWAY#
```

Observe que la dirección local externa y la dirección global externa son iguales. Esta dirección es la dirección de origen de red remota del ISP. Para que el ping del ISP se realice correctamente, la direcciónglobal interna de NAT estática 209.165.200.225 se tradujo a la dirección local interna de la PC-A (192.168.1.20).

f. Verifique las estadísticas de NAT mediante el **comando show ip nat statistics** en el router Gateway.

```
Gateway# show ip nat statistics
```

```
GATEWAY#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial1/0
Inside interfaces:
  FastEthernet0/0
Hits: 20  Misses: 10
CEF Translated packets: 30, CEF Punted packets: 0
Expired translations: 10
Dynamic mappings:
Appl doors: 0
Normal doors: 0
Queued Packets: 0
GATEWAY#
```

Parte 3. Configurar y verificar la NAT dinámica

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto. La NAT dinámica produce una asignación de varias direcciones a varias direcciones entre direcciones locales y globales.

Paso 1. Borrar las NAT

Antes de seguir agregando NAT dinámicas, borre las NAT y las estadísticas de la parte 2.

```
Gateway# clear ip nat translation*

Gateway# clear ip nat statistics
```

```
GATEWAY#clear ip nat translation *
GATEWAY#clear ip nat statistics
GATEWAY#
```

Paso 2. Definir una lista de control de acceso (ACL) que coincida con el rango de direcciones IP privadas de LAN

La ACL 1 se utiliza para permitir que se traduzca la red 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#access-list 1 permit 192.168.1.0 0.0.0.255
GATEWAY(config)#end
GATEWAY#copy running-config startup-config
*Mar  1 01:12:04.111: %SYS-5-CONFIG_I: Configured from console by console
GATEWAY#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
GATEWAY#
```

Paso 3. Verificar que la configuración de interfaces de NAT siga siendo válida

Emita el comando **show ip nat statistics** en el router Gateway para verificar la configuración NAT.

Paso 4. Definir el conjunto de direcciones IP públicas utilizables

```
Gateway(config)# ip nat pool public_access 209.165.200.242
209.165.200.254 netmask 255.255.255.224
```

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#$65.200.242 209.165.200.254  netmask 255.255.255.224
GATEWAY(config)#end
GATEWAY#copy running-config startup-config
*Mar  1 01:29:19.519: %SYS-5-CONFIG_I: Configured from console by console
GATEWAY#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
GATEWAY#
```

Paso 5. Definir la NAT desde la lista de origen interna hasta el conjunto externo

Nota: Recuerde que los nombres de conjuntos de NAT distinguen mayúsculas de minúsculas y elnombre del conjunto que se introduzca aquí debe coincidir con el que se usó en el paso anterior.

```
Gateway(config)# ip nat inside source list 1 pool public_access
```

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#ip nat inside source list 1 pool public_access
GATEWAY(config)#end
GATEWAY#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

*Mar  1 01:30:34.615: %SYS-5-CONFIG_I: Configured from console by console[OK]
GATEWAY#
```

Paso 6. Probar la configuración

a. En la PC-B, haga ping a la interfaz Lo0 (192.31.7.1) en el ISP. Si el ping falló, resuelva y corrija los problemas. En el router Gateway, muestre la tabla de NAT.

```
PC-B> ping 192.31.7.1
84 bytes from 192.31.7.1 icmp_seq=1 ttl=254 time=45.298 ms
84 bytes from 192.31.7.1 icmp_seq=2 ttl=254 time=45.250 ms
84 bytes from 192.31.7.1 icmp_seq=3 ttl=254 time=45.210 ms
84 bytes from 192.31.7.1 icmp_seq=4 ttl=254 time=45.225 ms
84 bytes from 192.31.7.1 icmp_seq=5 ttl=254 time=45.429 ms

PC-B>
```

```
Gateway# show ip nat translations
```

```
GATEWAY#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
icmp 209.165.200.242:54771 192.168.1.21:54771 192.31.7.1:54771 192.31.7.1:54771
icmp 209.165.200.242:55027 192.168.1.21:55027 192.31.7.1:55027 192.31.7.1:55027
icmp 209.165.200.242:55283 192.168.1.21:55283 192.31.7.1:55283 192.31.7.1:55283
icmp 209.165.200.242:55539 192.168.1.21:55539 192.31.7.1:55539 192.31.7.1:55539
icmp 209.165.200.242:55795 192.168.1.21:55795 192.31.7.1:55795 192.31.7.1:55795
--- 209.165.200.242    192.168.1.21       ---                ---
GATEWAY#
```

¿Cuál es la traducción de la dirección host local interna de la PC-B?
192.168.1.21 = 209.165.200.242

Cuando la PC-B envió un mensaje ICMP a la dirección 192.31.7.1 en el ISP, se agregó a la tabla una entrada de NAT dinámica en la que se indicó ICMP como el protocolo.

¿Qué número de puerto se usó en este intercambio ICMP?
54771 (puede variar)

b. En la PC-B, abra un explorador e introduzca la dirección IP del servidor web simulado ISP (interfaz Lo0). Cuando se le solicite, inicie sesión como **webuser** con la contraseña **webpass.**

c. Muestre la tabla de NAT.

```
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225      192.168.1.20       ---                ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80 192.31.7.1:80
--- 209.165.200.242    192.168.1.22       ---                ---
```

¿Qué protocolo se usó en esta traducción? Tcp

¿Qué números de puerto se usaron?

- **Interno:** 1038 a 1052
- **Exterior:** 80

¿Qué número de puerto bien conocido y qué servicio se usaron?

Puerto 80, www o http

d. Verifique las estadísticas de NAT mediante el comando **show ip nat statistics** en el router Gateway.

```
Gateway# show ip nat statistics
```

```
GATEWAY#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial1/0
Inside interfaces:
  FastEthernet0/0
Hits: 5  Misses: 5
CEF Translated packets: 10, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 1
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 1 (7%), misses 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
GATEWAY#
```

Paso 7. Eliminar la entrada de NAT estática

En el paso 7, se elimina la entrada de NAT estática y se puede observar la entrada de NAT.

a. Elimine la NAT estática de la parte 2. Introduzca **yes** (sí) cuando se le solicite eliminar entradas secundarias.

```
Gateway(config)# no ip nat inside source static 192.168.1.20
209.165.200.225
```

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#no ip nat inside source static 192.168.1.20 209.165.200.225
GATEWAY(config)#end
GATEWAY#copy running-config startup-config
Destination filename [startup-config]?
*Mar  1 01:43:16.675: %SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
GATEWAY#
```

Entrada estática en uso, ¿desea eliminar las entradas secundarias? [no]: **yes**

b. Borre las NAT y las estadísticas.

```
GATEWAY#clear ip nat translation *
GATEWAY#clear ip nat statistics
```

c. Haga ping al ISP (192.31.7.1) desde ambos hosts.

```
PC-A> ping 192.31.7.1
84 bytes from 192.31.7.1 icmp_seq=1 ttl=254 time=45.375 ms
84 bytes from 192.31.7.1 icmp_seq=2 ttl=254 time=45.275 ms
84 bytes from 192.31.7.1 icmp_seq=3 ttl=254 time=45.167 ms
84 bytes from 192.31.7.1 icmp_seq=4 ttl=254 time=45.332 ms
84 bytes from 192.31.7.1 icmp_seq=5 ttl=254 time=45.314 ms
```

```
PC-B> ping 192.31.7.1
84 bytes from 192.31.7.1 icmp_seq=1 ttl=254 time=45.180 ms
84 bytes from 192.31.7.1 icmp_seq=2 ttl=254 time=45.228 ms
84 bytes from 192.31.7.1 icmp_seq=3 ttl=254 time=45.294 ms
84 bytes from 192.31.7.1 icmp_seq=4 ttl=254 time=45.256 ms
84 bytes from 192.31.7.1 icmp_seq=5 ttl=254 time=45.289 ms
```

d. Muestre la tabla y las estadísticas de NAT.

Gateway# **show ip nat statistics**

```
GATEWAY#show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces:
  Serial1/0
Inside interfaces:
  FastEthernet0/0
Hits: 10  Misses: 10
CEF Translated packets: 20, CEF Punted packets: 0
Expired translations: 10
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 2 (15%), misses 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
GATEWAY#
```

Reflexión

1. ¿Por qué debe utilizarse la NAT en una red?

   Debido a que no hay suficientes direcciones IP públicas y evitar el costo de adquisición de estas que provengan de un ISP. NAT también funciona como medida de seguridad para ocultar las direcciones internas de las redes externas

2. ¿Cuáles son las limitaciones de NAT?

   - Una desventaja del uso de NAT se relaciona con el rendimiento de la red, en especial, en el caso de los protocolos en tiempo real como VoIP.

- NAT aumenta los retrasos de switching porque la traducción de cada dirección IPv4 dentro de los encabezados del paquete lleva tiempo. Al primer paquete siempre se aplica el switching de procesos por la ruta más lenta. El router debe revisar todos los paquetes para decidir si necesitan traducción. El router debe modificar el encabezado de IPv4 y, posiblemente, el encabezado TCP o UDP. El checksum del encabezado de IPv4, junto con el checksum de TCP o UDP, se debe volver a calcular cada vez que se realiza una traducción. Si existe una entrada de caché, el resto de los paquetes atraviesan la ruta de switching rápido; de lo contrario, también se retrasan.

- Se pierde el direccionamiento de extremo a extremo. Muchos protocolos y aplicaciones de Internet dependen del direccionamiento de extremo a extremo desde el origen hasta el destino. Algunas aplicaciones no funcionan con NAT.

- El uso de NAT también genera complicaciones para los protocolos de tunneling como IPsec, ya que NAT modifica los valores en los encabezados que interfieren en las verificaciones de integridad que realizan IPsec y otros protocolos de tunneling.

Conclusiones:

Cruz Chávez Alan Francisco:

En el desarrollo de la practica aplicamos los conocimientos sobre NAT estática y NAT dinámica donde se configuro desde los aspectos esenciales que deben tener nuestros router y swiches, con la NAT dinámica nos dimos cuenta que las traducciones no existen en la tabla NAT hasta que el router recibe tráfico que requiere traducción, mientras que en la NAT estática existe una tabla de traducciones que se configura con los comandos de NAT y no se borrara hasta que la NAT sea removida.

Gómez Salas Hugo Santiago:

Mendoza Rodríguez Israel:

Durante esta practica pusimos a prueba de NT estática y NAT dinámica, la nat estática nos permite conectar los equipos de una red interna para que puedan acceder a los servicios de un equipo externo como si estuvieran dentro de esta, mientras que una NAT dinámica permite que equipos externos accedan con un un mismo rango de direcciones que los equipos internos.

Ramírez Galindo Karina:

En esta práctica se verificó que la implementación de NAT permite interconectar redes con direcciones incompatibles, es decir, los equipos con direccionamiento privado, pueden acceder a una red externa con otro direccionamiento haciendo uso de NAT estático donde cada dirección y puerto se traducen igual y son fijadas por el administrador de la red o por NAT dinámico haciendo un pool de direcciones.