Laboratorio: Configurar NAT para IPv4

Topología

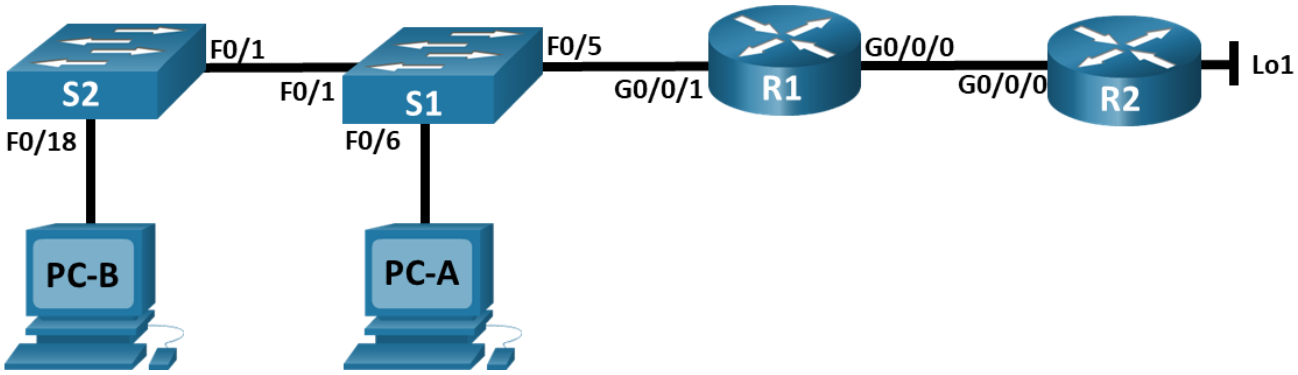

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/0/0	209.165.200.230	255.255.255.248
	G0/0/1	192.168.1.1	255.255.255.0
R2	G0/0/0	209.165.200.225	255.255.255.248
	Lo1	209.165.200.1	255.255.255.224
S1	VLAN 1	192.168.1.11	255.255.255.0
S2	VLAN 1	192.168.1.12	255.255.255.0
PC-A	NIC	192.168.1.2	255.255.255.0
PC-B	NIC	192.168.1.3	255.255.255.0

Objetivos

Parte 1: Armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: Configurar y verificar NAT para IPv4

Parte 3: Configurar y verificar PAT for IPv4

Parte 4: Configurar y verificar NAT estática para IPv4

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.

Un ISP asignó a una empresa el espacio de direcciones IP públicas 209.165.200.224/29. Esta red se utiliza para dirigir el enlace entre el router ISP (R2) y la puerta de enlace de la empresa (R1). La primera dirección

(209.165.200.225) se asigna a la interfaz g0/0/0 en R2 y la última dirección (209.165.200.230) se asigna a la interfaz g0/0/0 en R1. Las direcciones restantes (209.165.200.226-209.165.200.229) se utilizarán para proporcionar acceso a Internet a los anfitriones de la empresa. Se utiliza una ruta predeterminada de R1 a R2. El Internet se simula mediante una dirección de loopback en el router R2.

En este laboratorio, configurará varios tipos de NAT. Se probará, se verá y se verificará que se produzcan las traducciones y se interpretarán las estadísticas de NAT/PAT para controlar el proceso.

Nota: Los routers que se utilizan en los laboratorios prácticos de CCNA son Cisco 4221 con Cisco IOS XE versión 16.9.3 (imagen universalk9). Los switches utilizados en los laboratorios son Cisco Catalyst 2960s con Cisco IOS Release 15.2 (2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

Recursos necesarios

- 2 Router (Cisco 4221 con imagen universal Cisco IOS XE versión 16.9.3 o comparable)
- 2 Switches (Cisco 2960 con Cisco IOS versión 15.0(2), lanbasek9 image o comparable)
- 2 PC (Windows con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Instrucciones

Parte 1: Armar la red y configurar los ajustes básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos en los equipos host y los switches.

Paso 1: Realizar el cableado de red como se muestra en la topología

Conecte los dispositivos como se muestra en la topología y realice el cableado necesario.

Paso 2: Configure los parámetros básicos para cada router.

a. Asigne un nombre de dispositivo al router.

b. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.

c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

d. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.

e. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.

f. Cifre las contraseñas de texto sin formato.

g. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

h. Configure el direccionamiento IP de la interfaz como se especifica en la tabla anterior.

i. Configurar una ruta predeterminada desde R2 a R1.

j. Guardar la configuración en ejecución en el archivo de configuración de inicio

Paso 3: Configurar los parámetros básicos para cada switch

a. Asigne un nombre de dispositivo al switch.

b. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.

c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

d. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.

e. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.

f. Cifre las contraseñas de texto sin formato.

g. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

h. Cierre todas las interfaces que no se utilizarán.

i. Configure el direccionamiento IP de la interfaz como se especifica en la tabla anterior.

j. Guardar la configuración en ejecución en el archivo de configuración de inicio

Parte 2: Configurar y verificar NAT para IPv4.

En la Parte 2, configurará y verificará NAT para IPv4.

Paso 1: Configure NAT en R1 usando un grupo de tres direcciones, 209.165.200.226-209.165.200.228.

a. Configure una lista de acceso simple que defina qué hosts se van a permitir la traducción. En este caso, todos los dispositivos de la LAN R1 son elegibles para la traducción.

```
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

b. Cree el grupo NAT y asígnele un nombre y un rango de direcciones para usar.

```
R1(config)# ip nat pool PUBLIC_ACCESS 209.165.200.226 209.165.200.228 netmask
255.255.255.248
```

Nota: El parámetro netmask no es un delimitador de dirección IP. Debe ser la máscara de subred correcta para las direcciones asignadas, incluso si no está utilizando todas las direcciones de subred del grupo.

c. Configure la traducción, asociando la ACL y el Pool al proceso de traducción.

```
R1(config)# ip nat inside source list 1 pool PUBLIC_ACCESS
```

Nota: Tres puntos muy importantes. En primer lugar, la palabra 'inside' es crítica para el funcionamiento de este tipo de NAT. Si lo omite, NAT no funcionará. En segundo lugar, el número de lista es el número de ACL configurado en un paso anterior. El nombre del conjunto (distingue mayúsculas de minúsculas).

d. Define la interfaz interna.

```
R1(config)# interface g0/0/1
R1(config-if)# ip nat inside
```

e. Defina la interfaz externa.

```
R1(config)# interface g0/0/0
R1(config-if)# ip nat outside
```

Paso 2: Pruebe y verifique la configuración.

a. Desde PC-B, hacer ping a la interfaz Lo1 (209.165.200.1) en R2. Si el ping falló, resuelva y corrija los problemas. En R1, muestre la tabla NAT en R1 con el comando **show ip nat translations**.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
— 209.165.200.226 192.168.1.3 — —
icmp 209.165.200. 226:1 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:1
Total number of translations: 2
```

¿A qué se tradujo la dirección local interna de PC-B?

¿Qué tipo de dirección NAT es la dirección traducida?

b. Desde PC-A, hacer ping a la interfaz Lo1 (**209.165.200.1**) en R2. Si el ping falló, resuelva y corrija los problemas. En R1, muestre la tabla NAT en R1 con el comando **show ip nat translations.**

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
— 209.165.200.227 192.168.1.2 — —
— 209.165.200.226 192.168.1.3 — —
icmp 209.165.200. 227:1 192.168.1. 2:1 209.165.200. 1:1 209.165.200. 1:1
icmp 209.165.200. 226:1 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:1
Total number of translations: 7
```

c. Observe que la traducción anterior para PC-B todavía está en la tabla. Desde S1, hacer ping a la interfaz Lo1 (**209.165.200.1**) en R2. Si el ping falló, resuelva y corrija los problemas. En R1, muestre la tabla NAT en R1 con el comando **show ip nat translations**.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
— 209.165.200.227 192.168.1.2 — —
— 209.165.200.226 192.168.1.3 — —
— 209.165.200.228 192.168.1.11 — —
icmp 209.165.200. 226:1 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:1
icmp 209.165.200. 228:0 192.168.1. 11:0 209.165.200. 1:0 209.165.200. 1:0 209.165.200. 1:0
Total number of translations: 5
```

d. Ahora intenta hacer ping R2 Lo1 desde S2. Esta vez, las traducciones fallan y obtienes estos mensajes (o similares) en la consola R1:

```
Sep 23 15:43:55.562: %IOSXE-6-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000
TS:00000001473688385900 %NAT-6-ADDR_ALLOC_FAILURE: Address allocation failed; pool 1
may be exhausted [2]
```

e. Este es un resultado esperado, porque solo se asignan 3 direcciones, e intentamos hacer ping a Lo1 desde cuatro dispositivos. Recuerde que NAT es una traducción uno a uno. Entonces, ¿cuánto tiempo se asignan las traducciones? Ejecute el comando **show ip nat translations verbose** y verá que la respuesta es de 24 horas.

```
R1# show ip nat translations verbose
Pro Inside global Inside local Outside local Outside global
— 209.165.200.226 192.168.1.3 — —
  create: 09/23/19 15:35:27, use: 09/23/19 15:35:27, timeout: 23:56:42
  Id de mapa (In): 1
<output omitted>
```

f. Dado que el grupo está limitado a tres direcciones, NAT a un grupo de direcciones no es adecuado para nuestra aplicación. Borre las traducciones y estadísticas de NAT y pasaremos a PAT.

```
R1# clear ip nat translations *
R1# clear ip nat statistics
```

Parte 3: Configurar and verificar PAT for IPv4

En la Parte 3, configurará reemplazar NAT con PAT en un grupo de direcciones y, a continuación, con PAT utilizando una interfaz.

Paso 1: Elimine el comando de traducción en R1.

Los componentes de una configuración de traducción de direcciones son básicamente los mismos; algo (una lista de acceso) para identificar direcciones elegibles para ser traducidas, un grupo de direcciones configurado opcionalmente para traducirlas y los comandos necesarios para identificar las interfaces internas y externas. Desde la Parte 1, nuestra lista de acceso (lista de acceso 1) sigue siendo correcta para el escenario de la red, por lo que no es necesario volver a crearla. Vamos a utilizar el mismo grupo de direcciones, por lo que tampoco hay necesidad de recrear esa configuración. Además, las interfaces internas y externas no están cambiando. Para comenzar en la Parte 3, quite el comando que une la ACL y el grupo.

```
R1(config)# no ip nat inside source list 1 pool PUBLIC_ACCESS
```

Paso 2: Agregue el comando PAT en R1.

Ahora, configure para la traducción PAT a un grupo de direcciones (recuerde, la ACL y el Pool ya están configurados, por lo que este es el único comando que necesitamos para cambiar de NAT a PAT).

```
R1(config)# ip nat inside source list 1 pool PUBLIC_ACCESS overload
```

Paso 3: Pruebe y verifique la configuración.

a. Verifiquemos que la PAT está funcionando. Desde PC-B, hacer ping a la interfaz Lo1 (209.165.200.1) en R2. Si el ping falló, resuelva y corrija los problemas. En R1, muestre la tabla NAT en R1 con el comando **show ip nat translations.**

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200. 226:1 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:1
Total number of translations: 1 #
```

¿A qué se tradujo la dirección local interna de PC-B?

¿Qué tipo de dirección NAT es la dirección traducida?

¿Qué diferencia tiene la salida del comando **show ip nat translations** del ejercicio NAT?

b. Desde PC-A, hacer ping a la interfaz Lo1 (209.165.200.1) en R2. Si el ping falló, resuelva y corrija los problemas. En R1, muestre la tabla NAT en R1 con el comando **show ip nat translations.**

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200. 226:1 192.168.1. 2:1 209.165.200. 1:1 209.165.200. 1:1
Total number of translations: 1
```

Observe que sólo hay una traducción de nuevo. Envíe el ping una vez más y vuelva rápidamente al router y ejecute el comando **show ip nat translations verbose** y verá lo que pasó.

```
R1# show ip nat translations verbose
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200. 226:1 192.168.1. 2:1 209.165.200. 1:1 209.165.200. 1:1
  create: 09/23/19 16:57:22, uso: 09/23/19 16:57:25, timeout: 00:01:00
<output omitted>
```

Como puede ver, el tiempo de espera de traducción se ha reducido de 24 horas a 1 minuto.

c. Generar tráfico desde varios dispositivos para observar PAT. En PC-A y PC-B, utilice el parámetro -t con el comando ping para enviar un ping sin parar a la interfaz Lo1 de R2 (**ping -t 209.165.200.1**), luego vuelva a R1 y ejecute el comando **show ip nat translations**:

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200. 226:1 192.168.1. 2:1 209.165.200. 1:1 209.165.200. 1:1
icmp 209.165.200. 226:2 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:2
Total number of translations: 2
```

Observe que la dirección global interna es la misma para ambas sesiones.

¿Cómo realiza el router un seguimiento de qué respuestas van a dónde?

d. PAT to a pool es una solución muy eficaz para organizaciones pequeñas y medianas. Sin embargo, hay direcciones IPv4 no utilizadas involucradas en este escenario. Pasaremos a PAT con sobrecarga de interfaz para eliminar este desperdicio de direcciones IPv4. Detenga los pings en PC-A y PC-B con la combinación de teclas Control-C, luego borre las traducciones y las estadísticas de traducción:

```
R1# clear ip nat translations *
R1# clear ip nat statistics
```

Paso 4: En R1, elimine los comandos de traducción de nat pool.

Una vez más, nuestra lista de acceso (lista de acceso 1) sigue siendo correcta para el escenario de la red, por lo que no es necesario volver a crearla. Además, las interfaces internas y externas no están cambiando. Para comenzar con PAT en una interfaz, limpie la configuración eliminando el grupo NAT y el comando que une la ACL y el grupo.

```
R1(config)# no ip nat inside source list 1 pool PUBLIC_ACCESS overload
R1 (config) # sin ip nat pool PUBLIC_ACCESS
```

Paso 5: Agregue el comando de sobrecarga PAT especificando la interfaz externa.

Agregue el comando PAT que causará sobrecarga a la interfaz externa.

```
R1(config)# ip nat inside source list 1 interface g0/0/0 overload
```

Paso 6: Pruebe y verifique la configuración.

a. Vamos a verificar que PAT a la interfaz está funcionando. Desde PC-B, hacer ping a la interfaz Lo1 (209.165.200.1) en R2. Si el ping falló, resuelva y corrija los problemas. En R1, muestre la tabla NAT en R1 con el comando **show ip nat translations**.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200. 230:1 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:1
Total number of translations: 1
```

b. Generar tráfico desde varios dispositivos para observar PAT. En PC-A y PC-B, utilice el parámetro -t con el comando ping para enviar un ping sin parar a la interfaz Lo1 de R2 **(ping -t 209.165.200.1**). En S1 y S2, ejecute el comando ejecutivo privilegiado ping 209.165.200.1 repeat 2000. Luego regrese a R1 y ejecute el comando **show ip nat translations** .

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200. 230:3 192.168.1. 11:1 209.165.200. 1:1 209.165.200. 1:3
icmp 209.165.200. 230:2 192.168.1. 2:1 209.165.200. 1:1 209.165.200. 1:2
icmp 209.165.200. 230:4 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:4
icmp 209.165.200. 230:1 192.168.1. 12:1 209.165.200. 1:1 209.165.200. 1:1
Total number of translations: 4
```

Ahora todas las direcciones globales internas se asignan a la dirección IP de la interfaz g0/0/0.

Detén todos los pings. En PC-A y PC-B, utilizando la combinación de teclas CTRL-C.

Parte 4: Configurar y verificar NAT para IPv4.

En la Parte 4, configurará NAT estático para que PC-A sea directamente accesible desde Internet. PC-A será accesible desde R2 a través de la dirección 209.165.200.229.

Nota: La configuración que está a punto de completar no sigue las prácticas recomendadas para puertas de enlace conectadas a Internet. Este laboratorio omite por completo cuáles serían las prácticas de seguridad estándar para centrarse en una configuración exitosa de NAT estática. En un entorno de producción, la coordinación cuidadosa entre la infraestructura de la red y los equipos de seguridad sería fundamental para apoyar este requisito.

Paso 1: En R1, borre las traducciones y estadísticas actuales.

```
R1# clear ip nat translations *
R1# clear ip nat statistics
```

Paso 2: En R1, configure el comando NAT necesario para asignar estáticamente una dirección interna a una dirección externa.

Para este paso, configure una asignación estática entre 192.168.1.11 y 209.165.200.1 mediante el siguiente comando:

```
R1(config)# ip nat inside source static 192.168.1.2 209.165.200.229
```

Paso 3: Pruebe y verifique la configuración.

a. Vamos a verificar que la NAT estática está funcionando. En R1, muestre la tabla NAT en R1 con el comando **show ip nat translations**, y debería ver el mapeo estático.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
— 209.165.200.229 192.168.1.2 — —
Total number of translations: 1
```

b. La tabla de traducción muestra que la traducción estática está en vigor. Verifica esto haciendo ping desde R2 a 209.165.200.229. El comando ping debe funcionar.

Nota: es posible que tenga que desactivar el firewall de PC para que funcionen los pings.

c. En R1, muestre la tabla NAT en R1 con el comando **show ip nat translations**, y debería ver la asignación estática y la traducción a nivel de puerto para los pings entrantes.

```
R1# show ip nat translations
Pro Inside global Inside local Outside local Outside global
— 209.165.200.229 192.168.1.2 — —
icmp 209.165.200. 229:3 192.168.1. 2:3 209.165.200. 225:3 209.165.200. 225:3
Total number of translations: 2
```

Esto válida que la NAT estática está funcionando.

Tabla de resumen de interfaces de router

Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet #2	Interfaz serial #1	Interfaz serial #2
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Nota: Para conocer la configuración del router, observe las interfaces para identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, aunque puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo de esto. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS para representar la interfaz.