

Práctica de laboratorio: configuración de NAT dinámica y estática

Topología

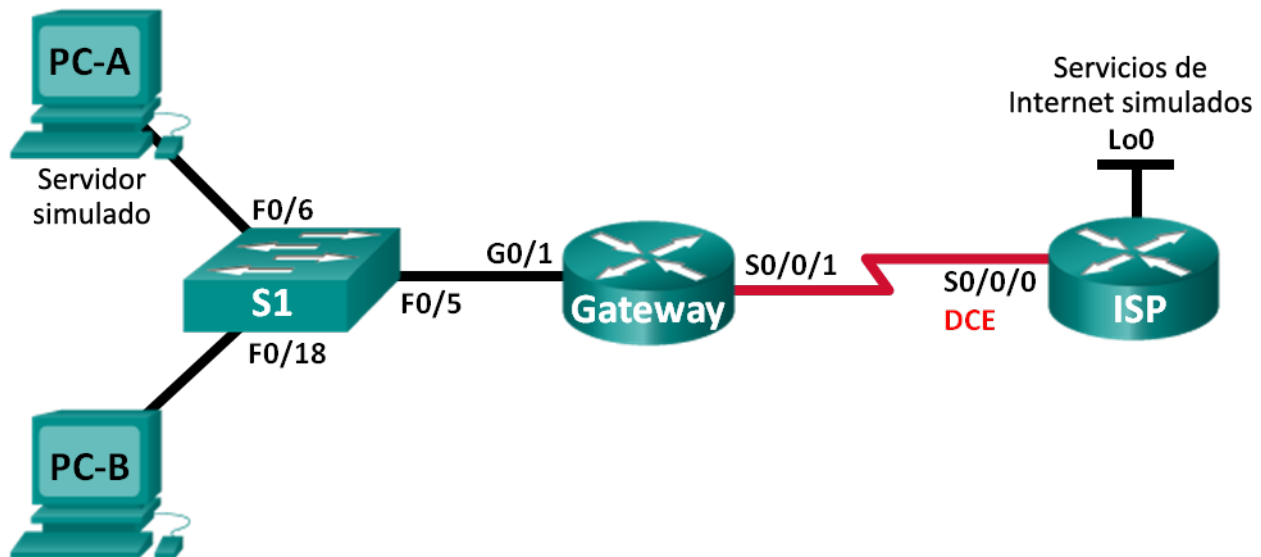


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
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

Información básica/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.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universal9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, 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 que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y el switch se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: armar la red y verificar la conectividad

En la parte 1, establecerá la topología de la red 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 el cableado de red tal como se muestra en la topología.

Conecte los dispositivos tal como se muestra en el diagrama de la topología y realice el cableado según sea necesario.

Paso 2: configurar los equipos host.

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

Paso 4: configurar los parámetros básicos para cada router.

- Desactive la búsqueda del DNS.
- Configure las direcciones IP para los routers como se indica en la tabla de direccionamiento.
- Establezca la frecuencia de reloj en **1280000** para las interfaces seriales DCE.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada del comando.

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
```

Paso 6: configurar el routing estático.

- a. Cree una ruta estática del router ISP al router Gateway usando el rango asignado de direcciones de red públicas 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

- 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
```

Paso 7: Guardar la configuración en ejecución en la configuración de inicio.

Paso 8: Verificar la conectividad de la red

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

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 tengan acceso a la PC-A desde Internet. 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
```

Paso 2: Especifique 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
```

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
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.225    192.168.1.20      ---                ---
```

¿Cuál es la traducción de la dirección host local interna?

192.168.1.20 = _____

¿Quién asigna la dirección global interna?

¿Quién asigna la dirección local interna?

- 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 los problemas. En el router Gateway, muestre la tabla de NAT.

```
Gateway# show ip nat translations
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
--- 209.165.200.225    192.168.1.20      ---                ---
```

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

¿Qué número de puerto se usó en este intercambio ICMP? _____

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 eliminado de la tabla de NAT.

¿Qué protocolo se usó para esta traducción? _____

¿Cuáles son los números de puerto que se usaron?

Global/local interno: _____

Global/local externo: _____

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

```
Gateway# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:12 192.168.1.20:12   209.165.201.17:12 209.165.201.17:12
--- 209.165.200.225    192.168.1.20      ---                ---
```

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 dirección

global 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
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39 Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

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
```

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
```

Paso 3: verificar que la configuración de interfaces 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
```

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 el nombre 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
```

Paso 6: probar la configuración.

- 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.

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

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
icmp	209.165.200.242:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
---	209.165.200.242	192.168.1.21	---	---

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

192.168.1.21 = _____

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? _____

- 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**.
- 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? _____

¿Qué números de puerto se usaron?

Interno: _____

Externo: _____

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

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

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345 Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
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 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

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
```

```
Static entry in use, do you want to delete child entries? [no]: yes
```

- b. Borre las NAT y las estadísticas.
- c. Haga ping al ISP (192.31.7.1) desde ambos hosts.
- d. Muestre la tabla y las estadísticas de NAT.

```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16 Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
```

```
[Id: 1] access-list 1 pool public_access refcount 4
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
```

```
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Gateway# **show ip nat translation**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.243:512	192.168.1.20:512	192.31.7.1:512	192.31.7.1:512
---	209.165.200.243	192.168.1.20	---	---
icmp	209.165.200.242:512	192.168.1.21:512	192.31.7.1:512	192.31.7.1:512
---	209.165.200.242	192.168.1.21	---	---

Nota: este es solo un resultado de muestra. Es posible que su resultado no coincida exactamente.

Reflexión

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

2. ¿Cuáles son las limitaciones de NAT?

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 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)
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)
<p>Nota: para conocer la configuración del router, observe las interfaces a fin de 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, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.</p>				