



NAT para IPv4

Enterprise Networking, Security,
and Automation (ENSA)



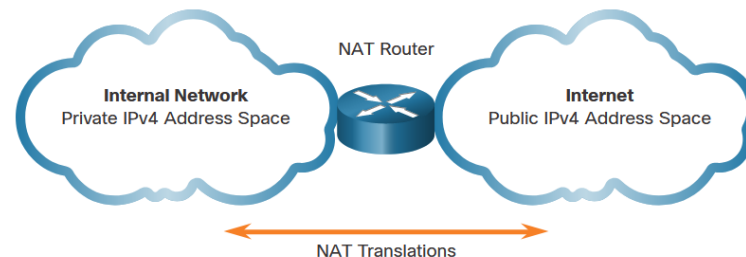
1. Características de NAT

Características de NAT

Espacio de direcciones IPv4

- Las redes suelen implementarse mediante el uso de direcciones IPv4 privadas, según se definen en RFC 1918.
- Las direcciones IPv4 privadas no se pueden enrutar a través de Internet y se usan dentro de una organización o sitio para permitir que los dispositivos se comuniquen localmente.
- Para permitir que un dispositivo con una dirección IPv4 privada acceda a recursos y dispositivos fuera de la red local, primero se debe traducir la dirección privada a una dirección pública.

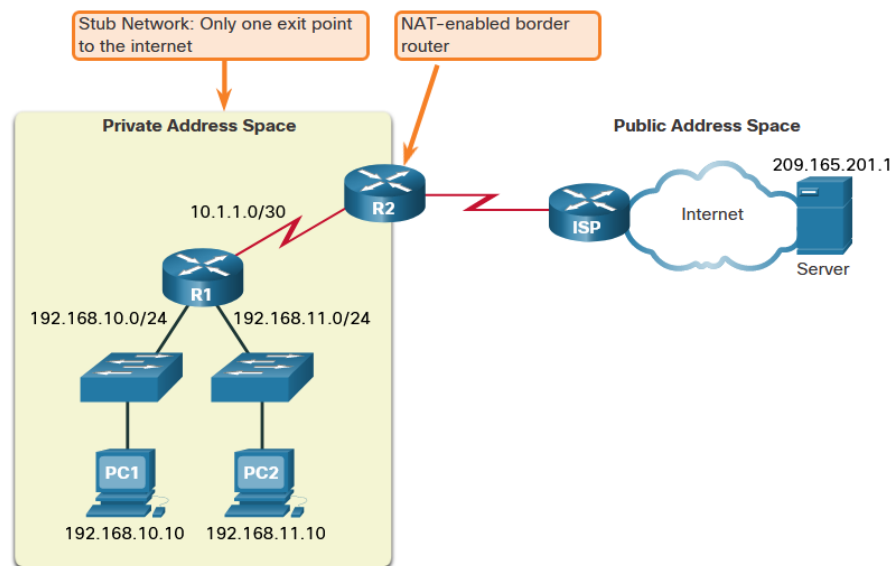
Clase	Rango	Rango
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16



Características de NAT

¿Qué es NAT?

- El uso principal de NAT es conservar las direcciones IPv4 públicas.
- Traduce direcciones IPv4 privadas a una dirección IP pública.
- NAT permite que las redes utilicen direcciones IPv4 privadas internamente y las traduce a una dirección pública cuando sea necesario.
- En general, los routers NAT funcionan en la frontera de una red de rutas internas.

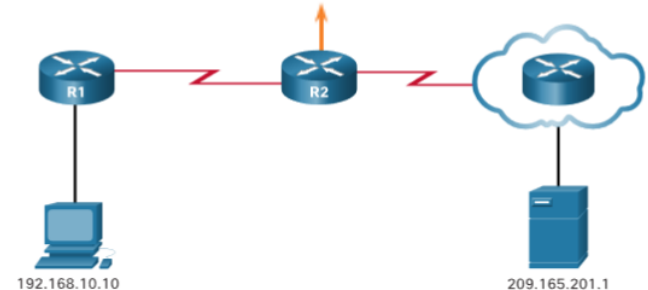


¿Cómo funciona es NAT?

PC1 quiere comunicarse con un servidor web externo con dirección pública 209.165.201.1.

1. La PC1 envía un paquete dirigido al servidor web.
2. R2 recibe el paquete y lee la dirección IPv4 de origen para determinar si necesita traducción.
3. R2 agrega la asignación de la dirección local a la global a la tabla NAT.
4. El R2 envía el paquete con la dirección de origen traducida hacia el destino.
5. El servidor web responde con un paquete dirigido a la dirección global interna de la PC1 (209.165.200.226).
6. El R2 recibe el paquete con la dirección de destino 209.165.200.226. El R2 revisa la tabla de NAT y encuentra una entrada para esta asignación. El R2 usa esta información y traduce la dirección global interna (209.165.200.226) a la dirección local interna (192.168.10.10), y el paquete se reenvía a la PC1.

NAT Table			
Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



Características de NAT

Terminología de NAT

NAT incluye cuatro tipos de direcciones:

- Dirección local interna.
- Dirección global interna.
- Dirección local externa.
- Dirección global externa.

La terminología NAT siempre se aplica desde la perspectiva del dispositivo con la dirección traducida:

- **Dirección interna** - La dirección del dispositivo que NAT está traduciendo.
- **Dirección externa** - La dirección del dispositivo de destino.
- **Dirección local** - Una dirección local es cualquier dirección que aparece en la parte interna de la red.
- **Dirección global** - Una dirección global es cualquier dirección que aparece en la parte externa de la red.

Características de NAT

Terminología de NAT (Cont.)

Dirección local interna

La dirección de la fuente vista desde dentro de la red. Normalmente, es una dirección IPv4 privada. La dirección local interna de PC1 es 192.168.10.10.

Direcciones globales internas

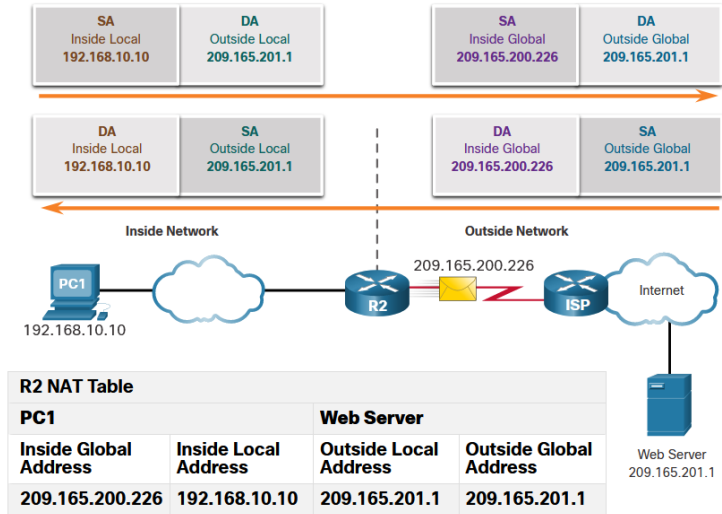
La dirección de origen vista desde la red externa. La dirección global interna de PC1 es 209.165.200.226

Dirección global externa

La dirección del destino vista desde la red externa. La dirección global externa del servidor web es 209.165.201.1

Dirección local externa

La dirección del destino como se ve desde la red interna. La PC1 envía tráfico al servidor web en la dirección IPv4 209.165.201.1. Si bien es poco frecuente, esta dirección podría ser diferente de la dirección globalmente enrutable del destino.



2. Tipos de NAT

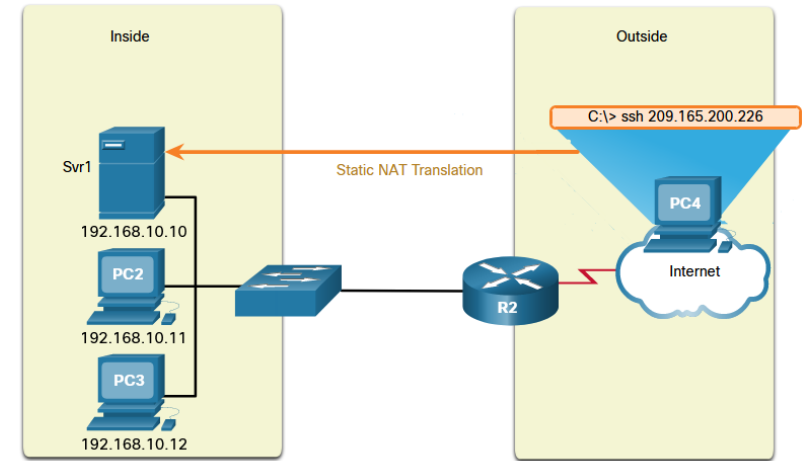
NAT estática

Tipos de NAT

NAT estático

La NAT estática utiliza una asignación uno a uno de direcciones locales y globales configuradas por el administrador de la red que permanecen constantes.

- La NAT estática es útil para servidores web o dispositivos que deben tener una dirección coherente a la que se pueda acceder desde Internet, como un servidor web de la empresa.
- También es útil para dispositivos que deben ser accesibles por personal autorizado cuando se encuentra fuera del sitio, pero no por el público en general en Internet.



Static NAT Table	
Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

Configurar NAT estático

Hay dos tareas básicas al configurar traducciones NAT estáticas:

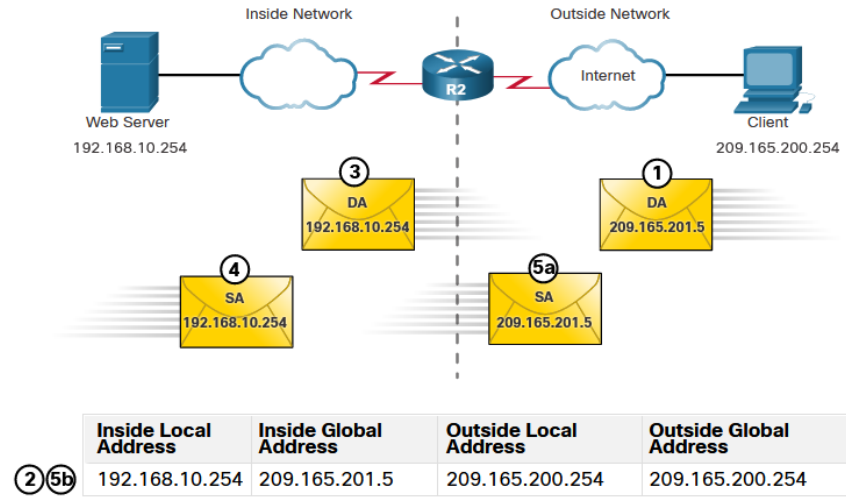
- **Paso 1** - Crear una asignación entre la dirección local interna y las direcciones globales internas utilizando el comando **ip nat inside source static**.
- **Paso 2** - Las interfaces que participan en la traducción se configuran como dentro o fuera en relación con NAT con los comandos **ip nat inside** y **ip nat outside**.

```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
R2(config)#
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

Analizar NAT estático

El proceso de traducción NAT estática entre el cliente y el servidor web:

1. El cliente envía un paquete al servidor web.
2. R2 recibe paquetes del cliente en su interfaz NAT externa y verifica su tabla NAT.
3. R2 traduce la dirección global interna de la dirección local interna y reenvía el paquete hacia el servidor web.
4. El servidor web recibe el paquete y responde al cliente utilizando su dirección local interna.
5. (a) R2 recibe el paquete del servidor web en su interfaz interna NAT con la dirección de origen de la dirección local interna del servidor web y (b) traduce la dirección de origen a la dirección global interna.



NAT estática

Verificación de NAT

Para verificar la operación NAT, emita el comando **show ip nat translation**.

- Este comando muestra las traducciones NAT activas.
- Debido a que el ejemplo es una configuración NAT estática, siempre figura una traducción en la tabla de NAT, independientemente de que haya comunicaciones activas.

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
- 209.165.201.5 192.168.10.254 - -
Total number of translations: 1
```

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 209.165.201.5 192.168.10.254 209.165.200.254 209.165.200.254 209.165.200.254
--- 209.165.201.5 192.168.10.254 --- ---
Total number of translations: 2
```

Verificación de NAT (Cont.)

Otro comando útil es **show ip nat stats**.

- Muestra información sobre el número total de traducciones activas, los parámetros de configuración de NAT, el número de direcciones en el grupo y el número de direcciones que se han asignado.
- Para verificar que la traducción NAT está funcionando, es mejor borrar las estadísticas de cualquier traducción anterior utilizando el comando **clear ip nat statistics** antes de realizar la prueba.

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 4 Misses: 1
(resultado omitido)
```

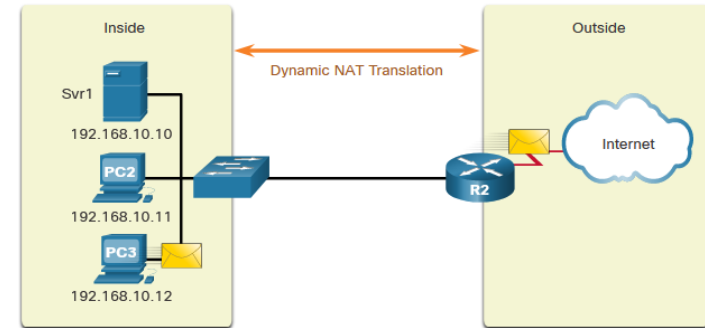
NAT dinámica

Tipos de NAT

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.
- Las otras direcciones del grupo todavía están disponibles para su uso.



IPv4 NAT Pool	
Inside Local Address	Inside Global Address Pool - Addresses reachable via R2
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

Configurar NAT dinámico

Hay cinco tareas para configurar las traducciones NAT estáticas.

- **Paso 1:** Defina el conjunto de direcciones que se utilizarán para la traducción con el comando **ip natpool**.
- **Paso 2** - Configure una ACL estándar para identificar (permitir) solo aquellas direcciones que se traducirán.
- **Paso 3** - Enlazar la ACL al grupo, utilizando el **comando ip nat inside source list**.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
```

Configurar NAT dinámico (Cont.)

Hay cinco tareas para configurar las traducciones NAT estáticas.

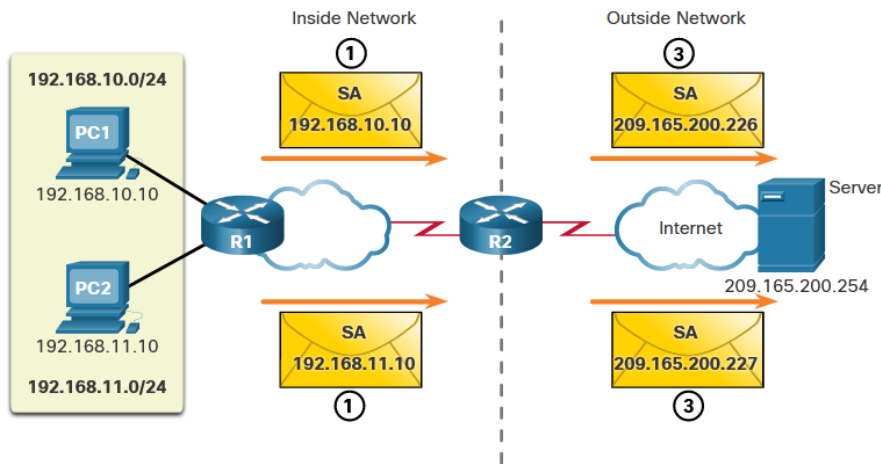
- **Paso 4** - Identifique qué interfaces están dentro.
- **Paso 5** - Identifique qué interfaces están fuera.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
R2(config-if)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

Analizar NAT dinámico: interior a exterior

Proceso de traducción de NAT dinámica:

1. PC1 y PC2 envían paquetes solicitando una conexión al servidor.
2. R2 recibe el primer paquete de PC1, comprueba el ALC para determinar si el paquete debe traducirse, selecciona una dirección global disponible y crea una entrada de traducción en la tabla NAT.
3. El R2 reemplaza la dirección de origen local interna de la PC1, 192.168.10.10, por la dirección global interna traducida 209.165.200.226 y reenvía el paquete. (El mismo proceso ocurre para el paquete de PC2 usando la dirección traducida de 209.165.200.227.)

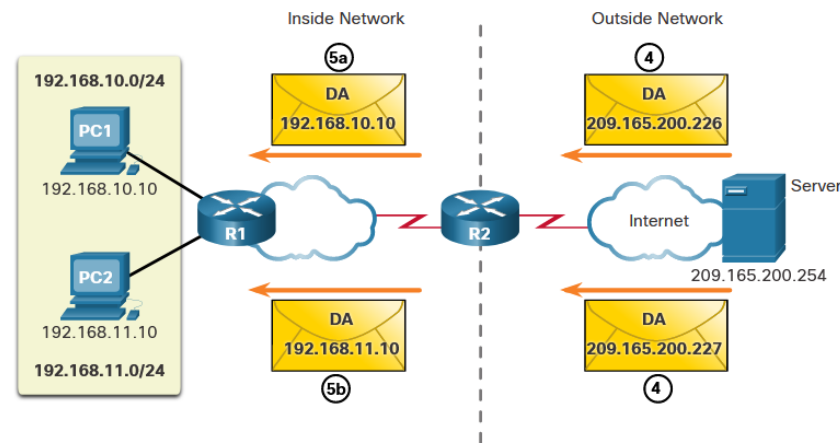


IPv4 NAT Pool	
Inside Local Address Pool	Inside Global Address
② 192.168.10.10	209.165.200.226
② 192.168.11.10	209.165.200.227

Analizar NAT dinámico: de exterior a interior

Proceso de traducción de NAT dinámica:

4. El servidor recibe el paquete de PC1 y responde con la dirección de destino 209.165.200.226. El servidor recibe el paquete de PC2, responde utilizando la dirección de destino 209.165.200.227.
5. (a) Cuando R2 recibe el paquete con la dirección de destino 209.165.200.226; realiza una búsqueda de tabla NAT y traduce la dirección de vuelta a la dirección local interna y reenvía el paquete hacia PC1.
(b) Cuando R2 recibe el paquete con la dirección de destino 209.165.200.227; realiza una búsqueda de tabla NAT y traduce la dirección de vuelta a la dirección local interior 192.168.11.10 y reenvía el paquete hacia PC2.

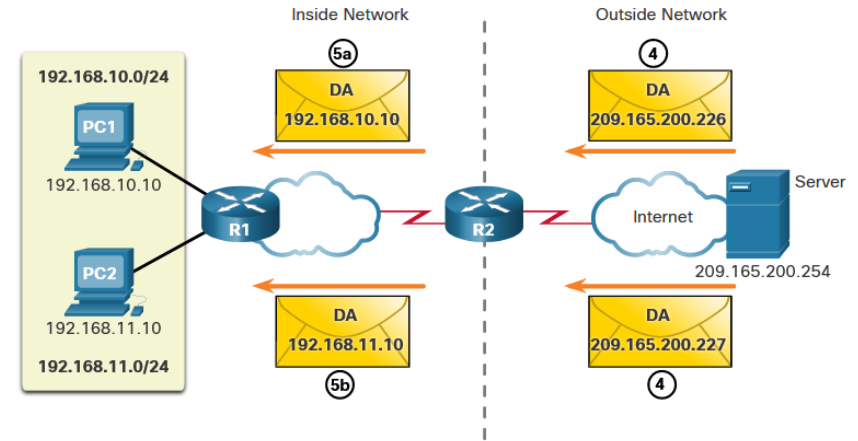


IPv4 NAT Pool	
Inside Local Address Pool	Inside Global Address
5a) 192.168.10.10	209.165.200.226
5b) 192.168.11.10	209.165.200.227

Analizar NAT dinámico: de exterior a interior (Cont.)

Proceso de traducción de NAT dinámica:

- La PC1 y la PC2 reciben los paquetes y continúan la conversación. El router lleva a cabo los pasos 2 a 5 para cada paquete.



IPv4 NAT Pool		
	Inside Local Address Pool	Inside Global Address
5a	192.168.10.10	209.165.200.226
5b	192.168.11.10	209.165.200.227

Verificar NAT dinámico

La salida del comando **show ip nat translation** muestra todas las traducciones estáticas que se han configurado y cualquier traducción dinámica que haya sido creada por el tráfico.

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.228 192.168.10.10 --- ---
- 209.165.200.229 192.168.11.10 - -
R2#
```

Verificar NAT dinámico (Cont.)

Si se agrega la palabra clave **verbose**, se muestra información adicional acerca de cada traducción, incluido el tiempo transcurrido desde que se creó y se utilizó la entrada.

```
R2# show ip nat translation verbose
Pro Inside global Inside local Outside local Outside global
tcp 209.165.200.228 192.168.10.10 --
    create 00:02:11, use 00:02:11 tiempo de espera: 86400000, left 23:57:48, Map Id (In): 1,
    flags:
none, use_count: 0, entry-id: 10, lc_entries: 0
tcp 209.165.200.229 192.168.11.10 --
    create 00:02:10, use 00:02:10 tiempo de espera: 86400000, left 23:57:49, Map Id (In): 1,
    flags:
none, use_count: 0, entry-id: 12, lc_entries: 0
R2#
```

Verificar NAT dinámico (Cont.)

El comando **show ip nat statistics** muestra información sobre el número total de traducciones activas, los parámetros de configuración de NAT, el número de direcciones en el grupo y cuántas de las direcciones se han asignado.

```
R2# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 0 extended)
Peak translations: 4, occurred 00:31:43 ago
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 47 Misses: 0
CEF Translated packets: 47, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 4
  pool NAT-POOL1: netmask 255.255.255.224
    inicio 209.165.200.226 fin 209.165.200.240
    type generic, total addresses 15, allocated 2 (13%), misses 0
(resultado omitido)
R2#
```


Verificar NAT dinámico (cont.)

El comando **show running-config** muestra los comandos NAT, ACL, interface o pool con los valores requeridos.

```
R2# show running-config | include NAT
ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
ip nat inside source list 1 pool NAT-POOL1
```

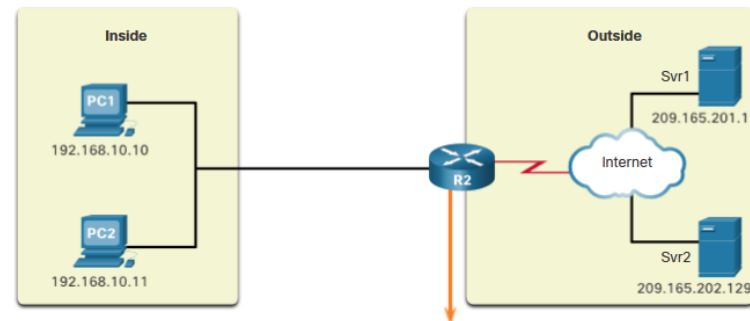
PAT

Tipos de NAT

Traducción de dirección de puerto

La traducción de la dirección del puerto (PAT), también conocida como “NAT con sobrecarga”, asigna varias direcciones IPv4 privadas a una única dirección IPv4 pública o a algunas direcciones.

- Con PAT, cuando el router NAT recibe un paquete del cliente, utiliza el número de puerto de origen para identificar de forma exclusiva la traducción NAT específica.
- PAT garantiza que los dispositivos usen un número de puerto TCP diferente para cada sesión con un servidor en Internet.



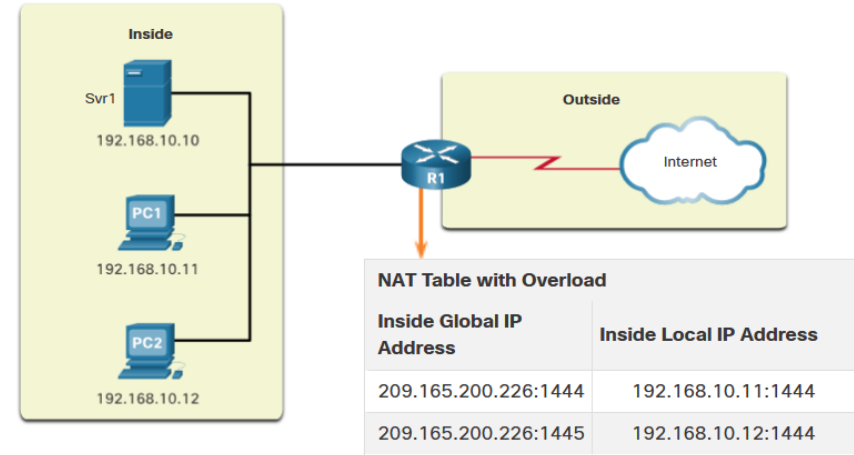
NAT Table with Overload			
Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

Tipos de NAT

Siguiente puerto disponible

PAT intenta conservar el puerto de origen inicial. Si el puerto de origen original ya está en uso, PAT asigna el primer número de puerto disponible a partir del comienzo del grupo de puertos apropiado 0-511, 512-1023 o 1024-65535.

- Cuando no hay más puertos disponibles y hay más de una dirección externa en el conjunto de direcciones, PAT avanza a la siguiente dirección para intentar asignar el puerto de origen inicial.
- El proceso continúa hasta que no haya más puertos disponibles o direcciones IPv4 externas en el grupo de direcciones.



Configurar PAT para usar una única dirección IPv4

Para configurar PAT para que utilice una sola dirección IPv4, agregue la palabra clave **overload** al comando **ip nat inside source** .

En el ejemplo, todos los hosts de la red 192.168.0.0/16 (coincidencia ACL 1) que envían tráfico a través del router R2 a Internet se traducirán a la dirección IPv4 209.165.200.225 (dirección IPv4 de la interfaz S0 / 1/0). Los flujos de tráfico se identificarán mediante números de puerto en la tabla NAT porque la palabra clave de **overload** está configurada.

```
R2(config)# ip nat inside source list 1 interface serial 0/1/0 overload
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2 (config) # interfaz serial0/1/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2 (config) # interfaz Serial0/1/1
R2(config-if)# ip nat outside
```

Configurar PAT para usar un grupo de direcciones

Un ISP puede asignar más de una dirección IPv4 pública a una organización. En este escenario, la organización puede configurar PAT para utilizar un grupo de direcciones públicas IPv4 para la traducción.

Para configurar PAT para un grupo de direcciones NAT dinámico, simplemente agregue la palabra clave **overload** al comando **ip nat inside source** .

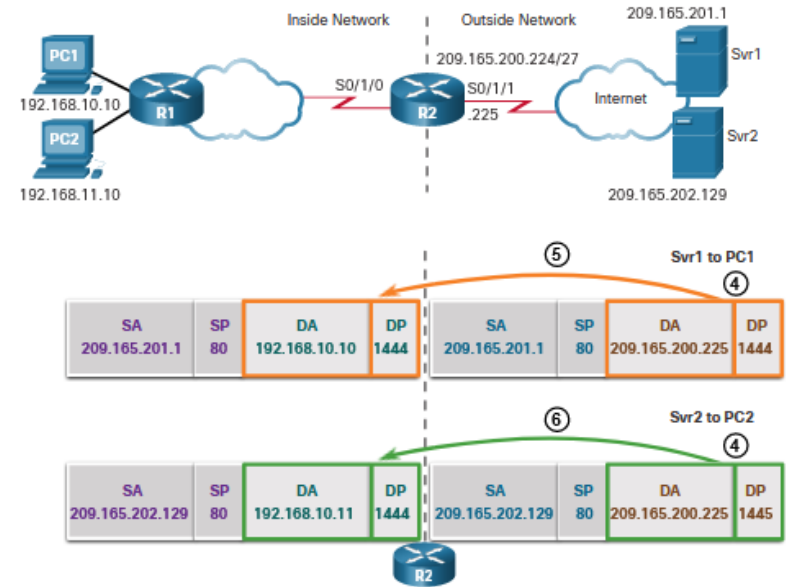
En el ejemplo, NAT-POOL2 está enlazado a una ACL para permitir la traducción de 192.168.0.0/16. Estos hosts pueden compartir una dirección IPv4 del grupo porque PAT está habilitado con la palabra clave **overload**.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
R2(config)# interface serial0/1/0
R2(config-if)# ip nat inside
R2 (config-if) # interfaz serial0/1/0
R2(config-if)# ip nat outside
```

PAT

Analizar PAT - Servidor a PC

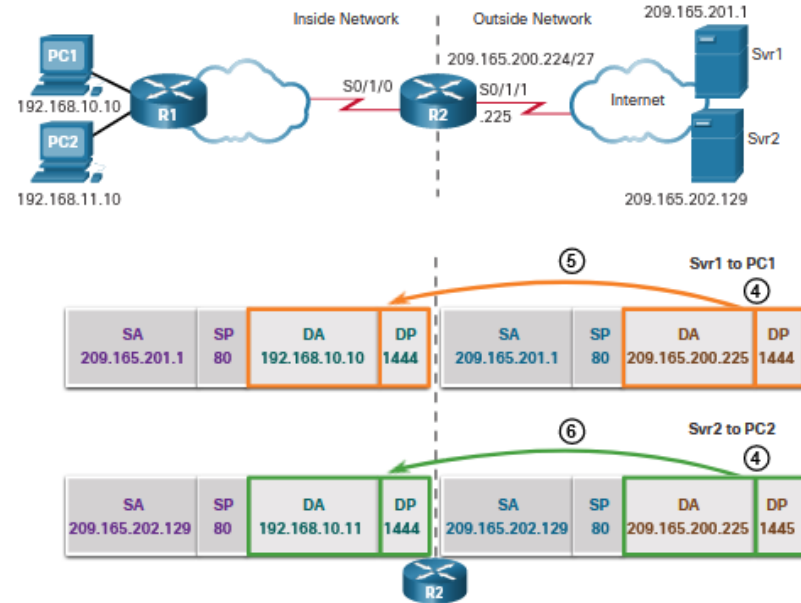
1. PC1 y PC2 envían paquetes a Svr1 y Svr2.
2. El paquete de la PC1 llega primero al R2. R2 modifica la dirección IPv4 de origen a 209.165.200.225 (dirección global interna). El paquete se reenvía a Svr1.
3. El paquete de la PC2 llega a R2. PAT cambia la dirección origen IPv4 de la PC2 a la dirección global interna 209.165.200.225. La PC2 tiene el mismo número de puerto de origen que la traducción para PC1. PAT aumenta el número de puerto de origen hasta que sea un valor único en su tabla. En este caso, 1445.



NAT Table			
Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.201.129:80	209.165.202.129:80

Analizar PAT - Servidor a PC

1. Los servidores usan el puerto de origen del paquete recibido como puerto de destino y la dirección de origen como dirección de destino para el tráfico de retorno.
2. R2 cambia la dirección IPv4 de destino del paquete de Srv1 de 209.165.200.225 a 192.168.10.10 y reenvía el paquete hacia PC1.
3. R2 cambia la dirección de destino del paquete de Srv2. de 209.165.200.225 a 192.168.10.11. y modifica el puerto de destino a su valor original de 1444. Luego, el paquete se reenvía hacia la PC2.



NAT Table			
Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.201.129:80	209.165.202.129:80

PAT Verificar PAT

Los mismos comandos utilizados para verificar NAT estático y dinámico se utilizan para verificar PAT. El comando **show ip nat translations** muestra las traducciones de dos hosts distintos a servidores web distintos. Observe que se asigna la misma dirección IPv4 209.165.200.226 (dirección global interna) a dos hosts internos distintos. Los números de puerto de origen en la tabla de NAT distinguen las dos transacciones.

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 209.165.200. 225:1444 192.168.10. 10:1444 209.165.201. 1:80
tcp 209.165.200. 225:1445 192.168.11. 10:1444 209.165.202. 129:80
R2#
```

Verificación PAT (cont.)

El comando **show ip nat statistics** verifica que NAT-POOL2 haya asignado una única dirección para ambas traducciones. También se muestra la cantidad y el tipo de traducciones activas, los parámetros de configuración de NAT, la cantidad de direcciones en el grupo y cuántas se han asignado.

```
R2# show ip nat statistics
Total active translations: 4 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:31:43 ago
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 4 Misses: 0
CEF Translated packets: 47, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
  pool NAT-POOL2: netmask 255.255.255.224
    start 209.165.200.225 end 209.165.200.240
    type generic, total addresses 15, allocated 1 (6%), misses 0
(resultado omitido)
R2#
```

