NAT

Índice

Introducción

No existen suficientes direcciones IPv4 públicas para asignar una dirección única a cada dispositivo conectado a Internet. Las redes suelen implementarse mediante el uso de direcciones IPv4 privadas, según se definen en RFC 1918.

Las direcciones privadas de Internet están definidas en RFC 1918:

Clase	Rango de direcciones internas RFC 1918	Prefijo CIDR
A	10.0.0.0 a 10.255.255.255	10.0.0.0/8
B	172.16.0.0 a 172.31.255.255	172.16.0.0/12
C	192.168.0.0 a 192.168.255.255	192.168.0.0/16

Estas direcciones privadas se utilizan dentro de una organización o un sitio para permitir que los dispositivos se comuniquen localmente. Sin embargo, como estas direcciones no identifican empresas u organizaciones individuales, las direcciones privadas IPv4 no se pueden enrutar a través de Internet. 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.

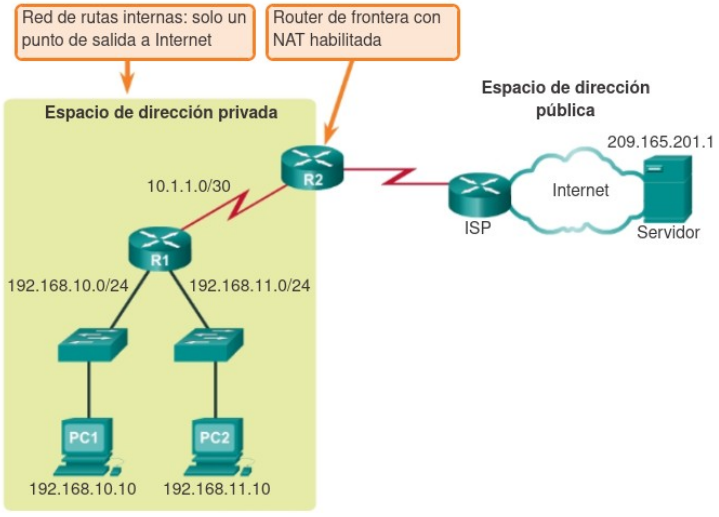
NAT proporciona la traducción de direcciones privadas a direcciones públicas. Esto permite que un dispositivo con una dirección IPv4 privada acceda a recursos fuera de su red privada, como los que se encuentran en Internet. La combinación de NAT con las direcciones IPv4 privadas resultó ser un método útil para preservar las direcciones IPv4 públicas. Se puede compartir una única dirección IPv4 pública entre cientos o incluso miles de dispositivos, cada uno configurado con una dirección IPv4 privada exclusiva.

Sin NAT, el agotamiento del espacio de direcciones IPv4 habría ocurrido mucho antes del año 2000. Sin embargo, NAT presenta algunas limitaciones. La solución es la transición final a IPv6.

Características de NAT

NAT tiene muchos usos, pero el principal es conservar las direcciones IPv4 públicas. Esto se logra al permitir que las redes utilicen direcciones IPv4 privadas internamente y al proporcionar la traducción a una dirección pública solo cuando sea necesario. NAT tiene el beneficio adicional de proporcionar cierto grado de privacidad y seguridad adicional a una red, ya que oculta las direcciones IPv4 internas de las redes externas.

Los routers con NAT habilitada se pueden configurar con una o más direcciones IPv4 públicas válidas. Estas direcciones públicas se conocen como “conjunto de NAT”. Cuando un dispositivo interno envía tráfico fuera de la red, el router con NAT habilitada traduce la dirección IPv4 interna del dispositivo a una dirección pública del conjunto de NAT. Para los dispositivos externos, todo el tráfico entrante y saliente de la red parece tener una dirección IPv4 pública del conjunto de direcciones proporcionado.



En general, los routers NAT funcionan en la frontera de una red de rutas internas. Una red de rutas internas es aquella que tiene una única conexión a su red vecina, una entrada hacia la red y una salida desde ella.

Cuando un dispositivo dentro de la red de rutas internas desea comunicarse con un dispositivo fuera de su red, el paquete se reenvía al router de frontera. El router de frontera realiza el proceso de NAT, es decir, traduce la dirección privada interna del dispositivo a una dirección pública, externa y enrutable.

Según la terminología de NAT, la red interna es el conjunto de redes sujetas a traducción. La red externa se refiere a todas las otras redes.

Al utilizar NAT, las direcciones IPv4 se designan de distinto modo, según si están en la red privada o en la red pública (Internet), y si el tráfico es entrante o saliente.

PC1 tiene la dirección local interna 192.168.10.10. Desde su perspectiva el servidor web tiene la dirección externa 209.165.201.1. Cuando se envían los paquetes del PC1 a la dirección global del servidor web, la dirección local interna del PC1 se traduce a 209.165.200.226 (dirección global interna). En general, la dirección del dispositivo externo no se traduce, ya que suele ser una dirección IPv4 pública.

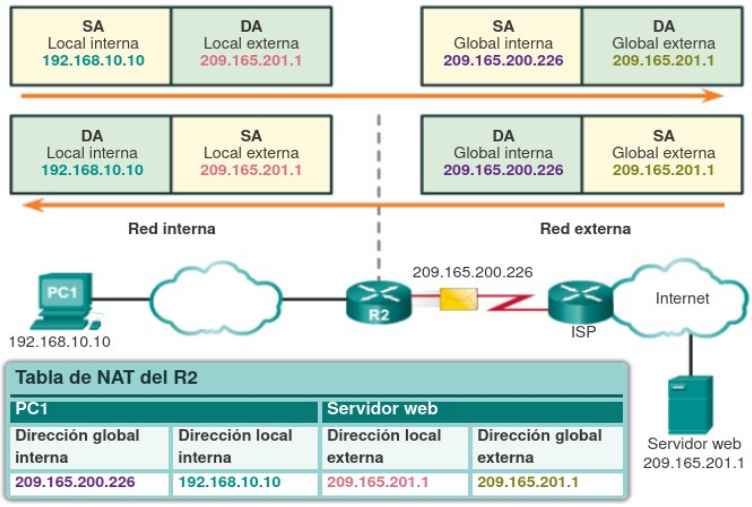


Tabla de NAT del R2

PC1		Servidor web	
Dirección global interna	Dirección local interna	Dirección local externa	Dirección global externa
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

Observa que el PC1 tiene distintas direcciones locales y globales, mientras que el servidor web tiene la misma dirección IPv4 pública en ambos casos. Desde la perspectiva del servidor web, el tráfico que se origina en el PC1 parece provenir de 209.165.200.226, la dirección global interna.

El router NAT, el R2 en la ilustración, es el punto de demarcación entre las redes internas y externas, así como entre las direcciones locales y globales.

Funcionamiento de NAT

En este ejemplo, el PC1 con la dirección privada 192.168.10.10 desea comunicarse con un servidor web externo con la dirección pública 209.165.201.1.

Cuando el paquete llega al router con NAT habilitada para la red, lee la dirección IPv4 de origen del paquete para determinar si este cumple con los criterios especificados para la traducción.

En este caso, la dirección IPv4 de origen cumple con los criterios y se traduce de 192.168.10.10 (dirección local interna) a 209.165.200.226 (dirección global interna). El router agrega esta asignación de dirección local a global a la tabla de NAT.

El servidor web responde con un paquete dirigido a la dirección global interna del PC1 (209.165.200.226) que es la IP externa o pública del router.

El router NAT recibe el paquete con la dirección de destino 209.165.200.226. Revisa la tabla de NAT y encuentra una entrada para esta asignación. El router 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 al PC1.

Tipos de NAT

Existen tres tipos de traducción NAT:

Traducción **estática** de direcciones (NAT estática): asignación de direcciones uno a uno entre una dirección local y una global.

Traducción **dinámica** de direcciones (NAT dinámica): asignación de varias direcciones a varias direcciones entre direcciones locales y globales.

Traducción de la dirección del **puerto** (PAT): asignación de varias direcciones a una dirección entre direcciones locales y globales. Este método también se conoce como “sobrecarga” (NAT con sobrecarga o NAPT).

NAT ESTÁTICA

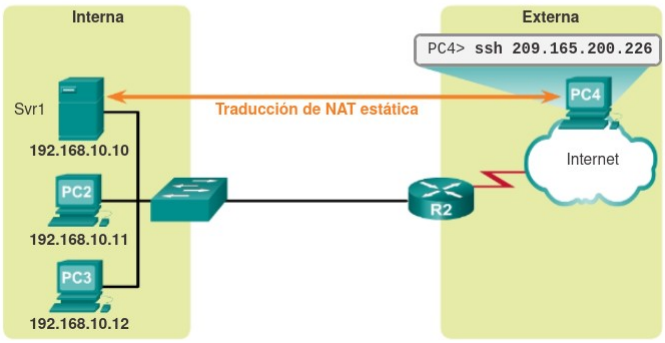
La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales. Estas asignaciones son configuradas por el administrador de red y se mantienen constantes.

En la ilustración, el R2 se configuró con las asignaciones estáticas para las direcciones locales internas del Svr1, PC2 y PC3. Cuando estos dispositivos envían tráfico a Internet, sus direcciones locales internas se traducen a las direcciones globales internas configuradas. Para las redes externas, estos dispositivos tienen direcciones IPv4 públicas.

NAT estática

Tabla de NAT estática

Dirección local interna	Dirección global interna: direcciones a las que se puede llegar a través del 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



La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener una dirección constante que sea accesible tanto desde Internet, como desde el servidor web de una empresa. También es útil para los dispositivos a los que debe poder acceder el personal autorizado cuando no está en su lugar de trabajo, pero no el público en general en Internet. Por ejemplo, un administrador de red puede acceder a la dirección global interna del Svr1 (209.165.200.226) desde la PC4 mediante SSH. El R2 traduce esta dirección global interna a la dirección local interna y conecta la sesión del administrador al Svr1.

La NAT estática requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.

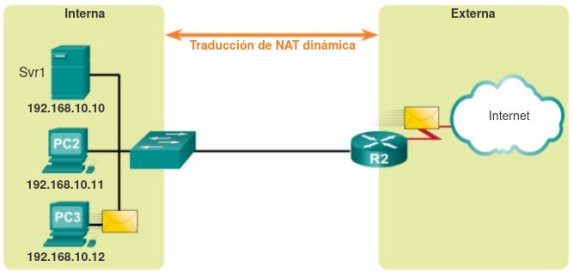
Nat Dinámica

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.

En la ilustración, la PC3 accede a Internet mediante la primera dirección disponible del conjunto de NAT dinámica. Las demás direcciones siguen disponibles para utilizarlas. Al igual que la NAT estática, la NAT dinámica requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.

NAT dinámica

Conjunto de NAT para IPv4	
Dirección local interna	**Conjunto de direcciones globales internas: direcciones a las que se puede llegar a través del R2**
192.168.10.12	209.165.200.226
Disponibles	209.165.200.227
Disponibles	209.165.200.228
Disponibles	209.165.200.229
Disponibles	209.165.200.230



NAPT o PAT

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. Esto es lo que hace la mayoría de los routers domésticos. El ISP asigna una dirección al router, no obstante, varios miembros del hogar pueden acceder a Internet de manera simultánea. Esta es la forma más común de NAT.

Con PAT, se pueden asignar varias direcciones a una o más direcciones, debido a que cada dirección privada también se rastrea con un número de puerto. Cuando un dispositivo inicia una sesión TCP/IP, genera un valor de puerto de origen TCP o UDP para identificar la sesión de forma exclusiva. Cuando el router NAT recibe un paquete del cliente, utiliza su 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 distinto para cada sesión con un servidor en Internet. Cuando llega una respuesta del servidor, el número de puerto de origen, que se convierte en el número de puerto de destino en la devolución, determina a qué dispositivo el router reenvía los paquetes. El proceso de PAT también valida que los paquetes entrantes se hayan solicitado, lo que añade un grado de seguridad a la sesión.

A medida que el R2 procesa cada paquete, utiliza un número de puerto (1331 y 1555, en este ejemplo) para identificar el dispositivo en el que se originó el paquete.

La dirección de origen (SA) es la dirección local interna a la que se agregó el número de puerto TCP/IP asignado. La dirección de destino (DA) es la dirección local externa a la que se agregó el número de puerto de servicio. En este ejemplo, el puerto de servicio es 80, que es HTTP.

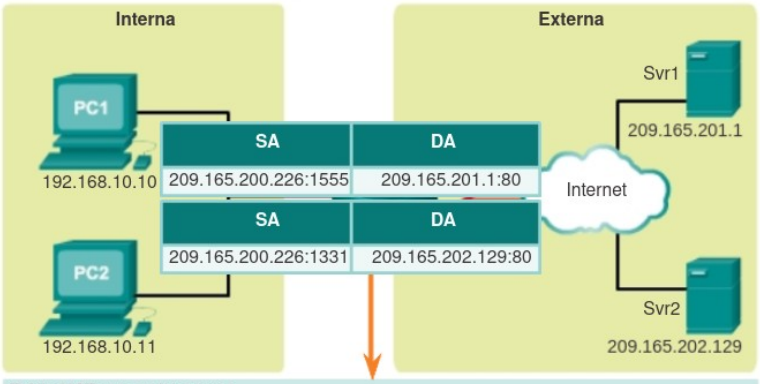


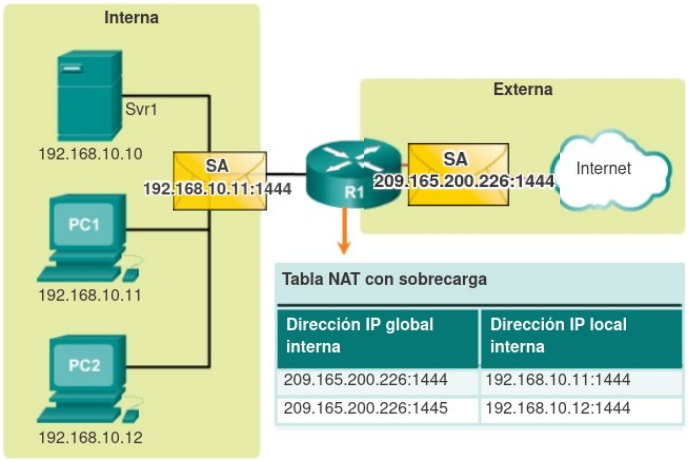
Tabla NAT con sobrecarga

Dirección IP global interna	Dirección IP local interna	Dirección IP local externa	Dirección IP global externa
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.10:1331	209.165.202.129:80	209.165.202.129:80

En el ejemplo anterior, los números de puerto del cliente, 1331 y 1555, no se modificaron en el router con NAT habilitada. Esta no es una situación muy probable, porque existe una gran posibilidad de que estos números de puerto ya se hayan conectado a otras sesiones activas.

PAT intenta conservar el puerto de origen inicial. Sin embargo, si el puerto de origen inicial ya está en uso, PAT asigna el primer número de puerto disponible desde el comienzo del grupo de puertos correspondiente de 0 a 511, 512 a 1023 o 1024 a 65 535. 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. Este proceso continúa hasta que no haya más direcciones IP externas o puertos disponibles.

En la figura de la derecha, los hosts eligieron el mismo número de puerto 1444. Esto resulta aceptable para la dirección interna, porque los hosts tienen direcciones IP privadas únicas. Sin embargo, en el router NAT, se deben cambiar los números de puerto; de lo contrario, los paquetes de dos hosts distintos saldrían del R2 con la misma dirección de origen. En este ejemplo, PAT asignó el siguiente puerto disponible (1445) a la segunda dirección host.

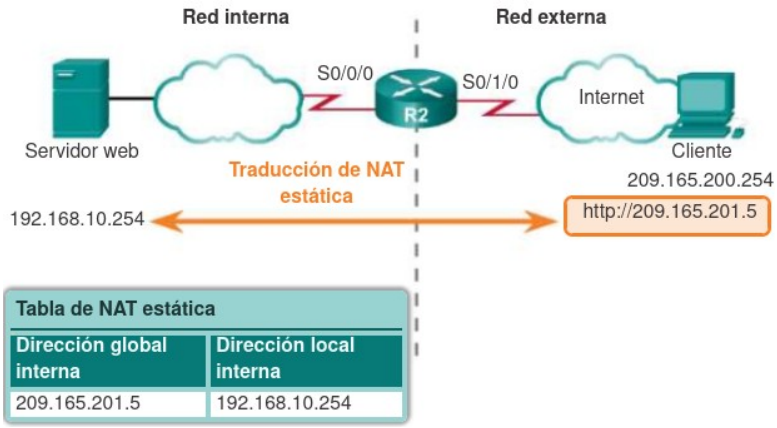


Configuración de NAT

Nat estática

La NAT estática es una asignación uno a uno entre una dirección interna y una dirección externa. La NAT estática permite que los dispositivos externos inicien conexiones a los dispositivos internos mediante la dirección pública asignada de forma estática. Por ejemplo, se puede asignar una dirección global interna específica a un servidor web interno de modo que se pueda acceder a este desde redes externas.

En el ejemplo se muestra una red interna que contiene un servidor web con una dirección IPv4 privada. El router R2 se configuró con NAT estática para permitir que los dispositivos en la red externa (Internet) accedan al servidor web. El cliente en la red externa accede al servidor web mediante una dirección IPv4 pública. La NAT estática traduce la dirección IPv4 pública a la dirección IPv4 privada.



Paso 1. El primer paso consiste en crear una asignación entre la dirección local interna y las direcciones globales internas. Por ejemplo, en la figura 1, la dirección local interna 192.168.10.254 y la dirección global interna 209.165.201.5 se configuraron como traducción NAT estática.

Se establece la traducción estática entre una dirección local interna y una dirección global interna.
`Router(config)# ip nat inside source static ip-local ip-global`

```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
```

Paso 2. Una vez configurada la asignación, las interfaces que participan en la traducción se configuran como interna o externa con respecto a NAT. En el ejemplo, la interfaz Serial 0/0/0 del R2 es una interfaz interna, y la interfaz Serial 0/1/0 es una interfaz externa.

Los paquetes que llegan hasta la interfaz interna del R2 (Serial 0/0/0) desde la dirección IPv4 local interna configurada (192.168.10.254) se traducen y, luego, se reenvían hacia la red externa. Los paquetes que llegan a la interfaz externa del R2 (Serial 0/1/0), que están dirigidos a la dirección IPv4 global interna configurada (209.165.201.5), se traducen a la dirección local interna (192.168.10.254) y, luego, se reenvían a la red interna.

Con la configuración que se muestra, el R2 traduce los paquetes del servidor web con la dirección 192.168.10.254 a la dirección IPv4 pública 209.165.201.5. El cliente de Internet dirige solicitudes web a la dirección IPv4 pública 209.165.201.5. El R2 reenvía ese tráfico al servidor web en 192.168.10.254.

Especificar la interfaz interna.
`Router(config)# interface tipo número`

Marque la interfaz como conectada al interior.
`Router(config-if)# ip nat inside`

Salga del modo de configuración de interfaz.
`Router(config-if)# exit`

Especificar la interfaz externa.
`Router(config)# interface tipo número`

Marque la interfaz como conectada al exterior.
`Router(config-if)# ip nat outside`

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
Identifies interface serial 0/0/0 as an inside NAT interface.
R2(config-if)# ip nat inside
R2(config-if)# exit

R2(config)# interface Serial0/1/0
R2(config-if)# ip address 209.165.200.225 255.255.255.224
Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config-if)# ip nat outside
```

Otros comandos

Con el comando **no ip nat inside source static** eliminamos la traducción

Router# show ip nat translations

Router# show ip nat statistics

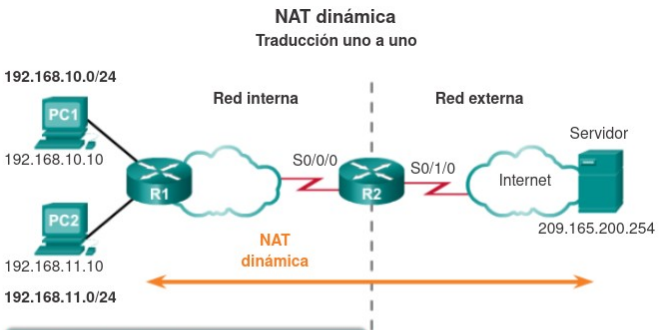
Router# clear ip nat statistics

Nat dinámica

Mientras que la NAT estática proporciona una asignación permanente entre una dirección local interna y una dirección global interna, la NAT dinámica permite la asignación automática de direcciones locales internas a direcciones globales internas. Por lo general, estas direcciones globales internas son direcciones IPv4 públicas. La NAT dinámica utiliza un grupo o un conjunto de direcciones IPv4 públicas para la traducción.

Al igual que la NAT estática, la NAT dinámica requiere que se configuren las interfaces interna y externa que participan en la NAT. Sin embargo, mientras que **la NAT estática crea una asignación permanente a una única dirección, la NAT dinámica utiliza un conjunto de direcciones**.

La topología de ejemplo que se muestra en la ilustración tiene una red interna que usa direcciones del espacio de direcciones privadas definido en RFC 1918. Hay dos LAN conectadas al router R1: 192.168.10.0/24 y 192.168.11.0/24. El router R2, es decir, el router de frontera, se configuró para NAT dinámica con un conjunto de direcciones IPv4 públicas de 209.165.200.226 a 209.165.200.240.



Conjunto de NAT para IPv4

Dirección global interna	Conjunto de direcciones locales internas
209.165.200.226	192.168.10.10
209.165.200.227	192.168.11.10
209.165.200.228	Disponibles
…	…
209.165.200.240	Disponibles

El conjunto de direcciones IPv4 públicas (conjunto de direcciones globales internas) se encuentra disponible para cualquier dispositivo en la red interna según el orden de llegada. Con la NAT dinámica, una única dirección interna se traduce a una única dirección externa. Con este tipo de traducción, debe haber suficientes direcciones en el conjunto para admitir a todos los dispositivos internos que necesiten acceso a la red externa al mismo tiempo. Si se utilizaron todas las direcciones del conjunto, los dispositivos deben esperar que haya una dirección disponible para poder acceder a la red externa.

Paso 1. Definir el conjunto de direcciones que se utilizará para la traducción con el comando **ip nat pool**. Por lo general, este conjunto es un grupo de direcciones públicas. Las direcciones se definen indicando la primera y la última dirección IP del conjunto. Las palabras clave netmask o prefix-length indican qué bits de la dirección pertenecen a la red y cuáles al host en el rango de direcciones.

Definir el conjunto de direcciones globales que se debe usar para la traducción.

```
ip nat pool nombre primera-ip última-ip
{netmask máscara-red | prefix-length longitud-
prefijo}
```

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226
209.165.200.240 netmask 255.255.255.224
```

Paso 2. Configurar una ACL estándar para identificar (permitir) solo aquellas direcciones que se deben traducir. Una ACL demasiado permisiva puede generar resultados impredecibles.

Configurar una lista de acceso estándar que permita las direcciones que se deben traducir.
access-list *número-lista-acceso* **permit** *origen* [*wildcard-origen*]

Recuerda que al final de cada ACL hay una instrucción implícita para denegar todo.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Paso 3. Conectar la ACL al conjunto. Para conectar la ACL al conjunto, se utiliza el comando **ip nat inside source list número-lista-acceso number pool nombre-conjunto**. El router utiliza esta configuración para determinar qué dirección (pool) recibe cada dispositivo (list).

Especificar la lista de acceso y el conjunto que se definieron en los pasos anteriores para establecer la traducción dinámica de origen.
ip nat inside source list *número-lista-acceso* **pool** *nombre*

```
R2(config)# ip nat inside source list 1 pool NAT-POOL1
```

Paso 4. Identificar qué interfaces son internas con respecto a NAT; es decir, cualquier interfaz que se conecte a la red interna y qué interfaces son externas con respecto a NAT; es decir, cualquier interfaz que se conecte a la red externa. Para ello utilizamos **ip nat inside | outside** como antes

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

Otros comandos

Router# show ip nat translations

Router# clear ip nat translation * borra todas las entradas

Router# clear ip nat translation inside ip-global ip-local borra la entrada que se especifica

Router# show ip nat statistics

Router# clear ip nat statistics

PAT

PAT (también denominada “NAT con sobrecarga”) conserva las direcciones del conjunto de direcciones globales internas al permitir que el router use una dirección global interna para muchas direcciones locales internas. El router mantiene información acerca de puertos TCP o UDP, por ejemplo, para volver a traducir la dirección global interna a la dirección local interna correcta. Cuando se asignan varias direcciones locales internas a una dirección global interna, los números de puerto TCP o UDP de cada host interno distinguen entre las direcciones locales.

Existen dos formas de configurar PAT, según cómo el ISP asigna las direcciones IPv4 públicas. En primer lugar, el ISP asigna más de una dirección IPv4 pública a la organización y, en segundo lugar, asigna una única dirección IPv4 pública que se requiere para que la organización se conecte al ISP.

Configuración de PAT para un conjunto de direcciones IP públicas

Si se emitió más de una dirección IPv4 pública para un sitio, estas direcciones pueden ser parte de un conjunto utilizado por PAT. Esto es similar a la NAT dinámica, con la excepción de que no existen suficientes direcciones públicas para realizar una asignación uno a uno entre direcciones internas y externas. Una gran cantidad de dispositivos comparte el pequeño conjunto de direcciones.

Aquí se muestran los pasos para configurar PAT a fin de que utilice un conjunto de direcciones. La diferencia principal entre esta configuración y la configuración para NAT dinámica uno a uno es que se utiliza la palabra clave overload. La palabra clave overload habilita PAT.

La configuración de ejemplo que se muestra más abajo establece la traducción de sobrecarga para el conjunto de NAT denominado NAT-POOL2. NAT-POOL2 contiene las direcciones de 209.165.200.226 a 209.165.200.240. Los hosts en la red 192.168.0.0/16 están sujetos a traducción. La interfaz S0/0/0 se identifica como interfaz interna, y la interfaz S0/1/0 se identifica como interfaz externa.

ip nat pool *nombre primera-ip última-ip* {**netmask** *máscara-red* | **prefix-length** *longitud-prefijo*}

Definir una lista de acceso estándar que permita las direcciones que se deben traducir.

access-list *número-lista-acceso* **permit** *origen* [*wildcard-origen*]

Especificar la lista de acceso y el conjunto que se definieron en los pasos anteriores para establecer la traducción de sobrecarga.

ip nat inside source list *número-lista-acceso* **pool** *nombre* **overload**

Identificar la interfaz interna.

interface *tipo número*
ip nat inside

Identificar la interfaz externa.

interface *tipo número*
ip nat outside

```
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 Serial0/0/0
R2(config-if)# ip nat inside
```

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

Configuración de PAT para una única dirección IPv4 pública

En el ejemplo, todos los hosts de la red 192.168.0.0/16 (que coincide con la ACL 1) que envían tráfico a Internet a través del router R2 se traducen a la dirección IPv4 209.165.200.225 (dirección IPv4 de la interfaz S0/1/0). Los flujos de tráfico se identifican por los números de puerto en la tabla de NAT, ya que se utilizó la palabra clave overload.

Si solo hay una única dirección IPv4 pública disponible, la configuración de sobrecarga generalmente asigna la dirección pública a la interfaz externa que se conecta al ISP. Todas las direcciones internas se traducen a la única dirección IPv4 cuando salen de la interfaz externa.

Paso 1. Definir una ACL para permitir que se traduzca el tráfico.

Paso 2. Configurar la traducción de origen con las palabras clave interface y overload. La palabra clave **interface** identifica la dirección IP de la interfaz que se debe utilizar en la traducción de las direcciones internas. La palabra clave **overload** le indica al router que realice un seguimiento de los números de puerto con cada entrada de NAT.

Básicamente es lo mismo que la anterior pero en vez de poner el pool ponemos la interface

Paso 3. Identificar cuáles son las interfaces internas con respecto a NAT. Es decir, toda interfaz que se conecte a la red interna y cuál es la interfaz externa con respecto a NAT. Esta debe ser la misma interfaz identificada en la instrucción de la traducción de origen del paso 2.

Definir una lista de acceso estándar que permita las direcciones que se deben traducir.

```
access-list número-lista-acceso permit origen
[wildcard-origen]
```

Especificar las opciones de ACL, interfaz de salida y sobrecarga para establecer la traducción dinámica de origen.

```
ip nat inside source list número-lista-acceso
interface tipo número overload
```

Identifique la interfaz interna.

```
interface type number
ip nat inside
```

Identifique la interfaz externa.

```
interface type number
ip nat outside
```

La configuración es similar a la de NAT dinámica, excepto que, en lugar de un conjunto de direcciones, se utiliza la palabra clave interface para identificar la dirección IPv4 externa. Por lo tanto, no se define ningún pool de NAT.

Otros comandos

Router# show ip nat translations

Router# show ip nat statistics

Router# clear ip nat statistics

Tunneling o reenvío de puertos

Consiste en reenviar el tráfico dirigido a un puerto de red específico desde un nodo de red hacia otro. Esta técnica permite que un usuario externo alcance un puerto en una dirección IPv4 privada (dentro de una LAN) desde el exterior a través de un router con NAT habilitada.

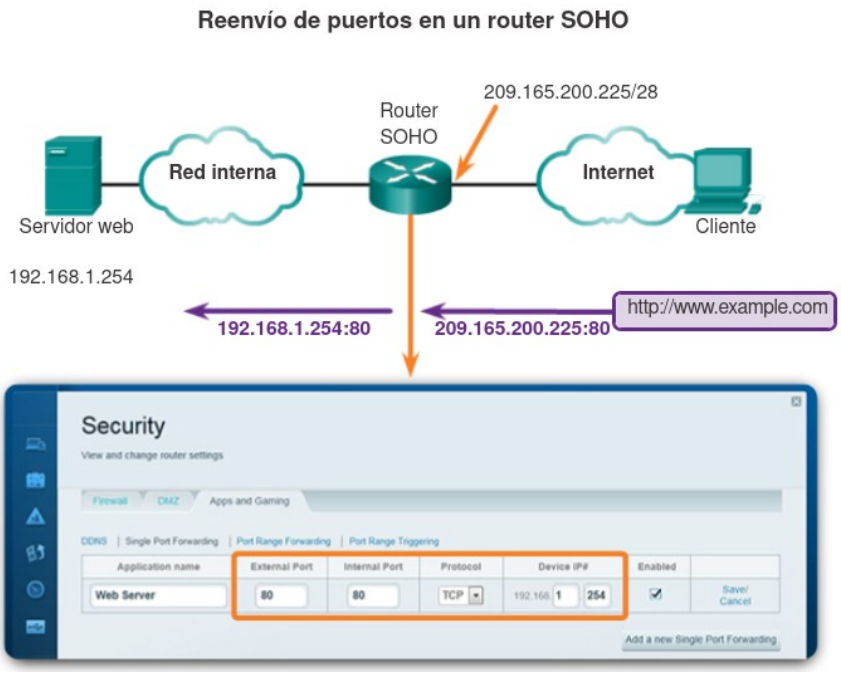
En general, las operaciones y los programas peer-to-peer para compartir archivos, como las aplicaciones de servidores web y los FTP salientes, requieren que los puertos de router se reenvíen o se abran para permitir que estas aplicaciones funcionen. Debido a que NAT oculta las direcciones internas, la comunicación peer-to-peer solo funciona desde adentro hacia fuera donde NAT puede asignar las solicitudes salientes a las respuestas entrantes.

El problema es que NAT no permite las solicitudes iniciadas desde el exterior. Esta situación se puede resolver de forma manual. El reenvío de puertos se puede configurar para identificar los puertos específicos que se pueden reenviar a los hosts internos.

Recuerda que las aplicaciones de software de Internet interactúan con los puertos de usuario que necesitan estar abiertos o disponibles para dichas aplicaciones. Las distintas aplicaciones usan puertos diferentes. Esto hace que las aplicaciones y los routers identifiquen los servicios de red de manera predecible. Por ejemplo, HTTP funciona a través del puerto bien conocido 80. Cuando alguien introduce la dirección http://www.iesrodeira.com, el explorador muestra el sitio web del IES de Rodeira. Ten en cuenta que no es necesario especificar el número de puerto HTTP para la solicitud de página, ya que la aplicación asume que se trata del puerto 80.

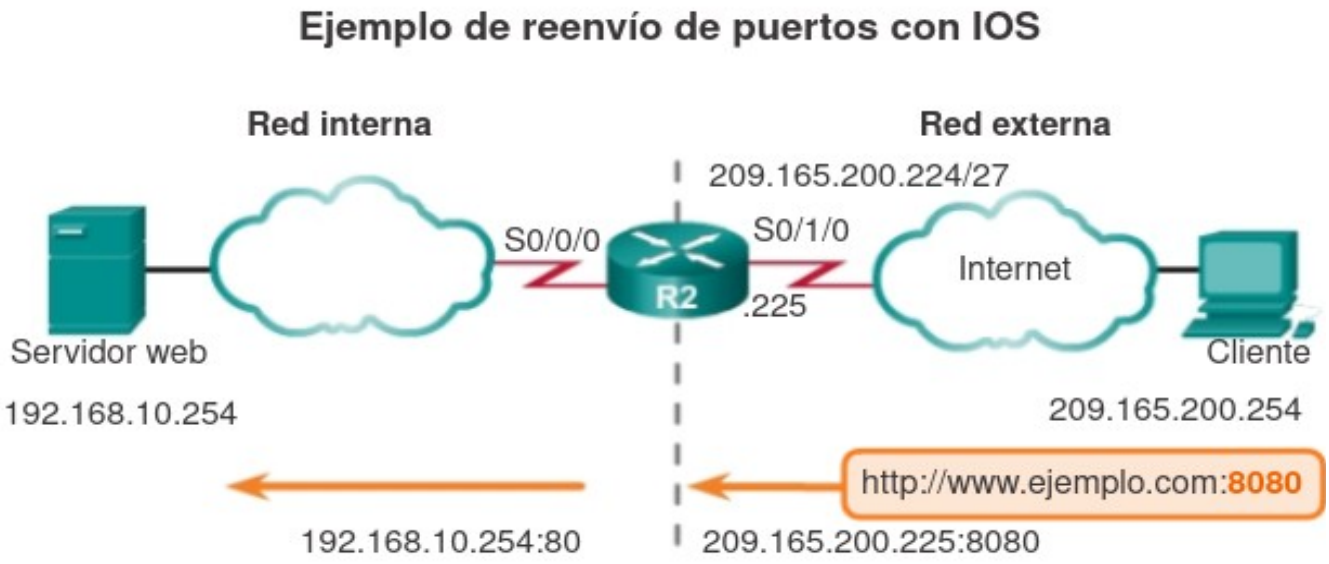
Si se requiere un número de puerto diferente, se puede agregar al URL separado por dos puntos (:). Por ejemplo, si el servidor web escuchara en el puerto 8080, el usuario escribiría http://www.ejemplo.com:8080.

El reenvío de puertos permite que los usuarios en Internet accedan a los servidores internos mediante el uso de la dirección de puerto de WAN del router y del número de puerto externo que coincida. En general, los servidores internos se configuran con direcciones IPv4 privadas definidas en RFC 1918. Cuando se envía una solicitud a la dirección IPv4 del puerto de WAN a través de Internet, el router reenvía la solicitud al servidor correspondiente en la LAN. Por motivos de seguridad, los routers de banda ancha no permiten que se reenvíe ninguna solicitud de redes externas a un host interno de manera predeterminada.



Se puede especificar un puerto distinto al puerto predeterminado 80. Sin embargo, el usuario externo tendría que saber el número de puerto específico que debe utilizar. Para especificar un puerto diferente, se modifica el valor del campo External Port Forwarding (Reenvío de puerto único).

Los comandos de IOS que se usan para implementar el reenvío de puertos son similares a los que se usan para configurar la NAT estática. Básicamente, el reenvío de puertos es una traducción de NAT estática con un número de puerto TCP o UDP específico.



Establece la traducción estática entre una dirección local interna y un puerto local, y entre una dirección global interna y un puerto global.

```
R2(config)# ip nat inside source static tcp
192.168.10.254 80 209.165.200.225 8080
```

Identifica la interfaz serial 0/0/0 como interfaz NAT interna.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identifica la interfaz serial 0/1/0 como interfaz NAT externa.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

Otros comandos

debug ip nat

debug ip nat detailed

nos provén de información sobre cada paquete que traduce el router.