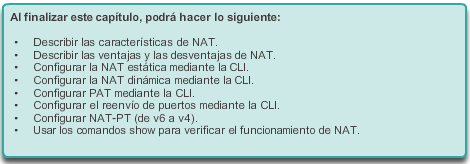
# Traducción de direcciones de red para IPv4 NAT.

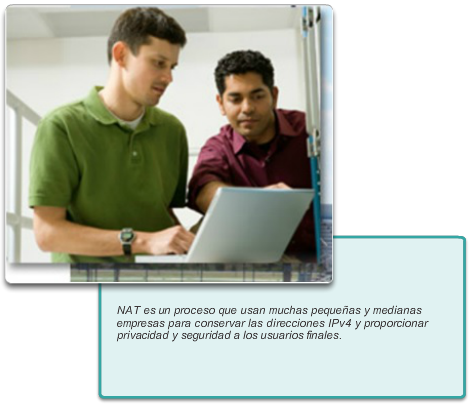
## Introducción

Todas las direcciones IPv4 públicas que se usan en Internet deben registrarse en un registro regional de Internet (RIR). Las organizaciones pueden arrendar direcciones públicas de un SP, pero solo el titular registrado de una dirección pública de Internet puede asignar esa dirección a un dispositivo de red. Sin embargo, con un máximo teórico de 4300 millones de direcciones, el espacio de direcciones IPv4 es muy limitado. Cuando Bob Kahn y Vint Cerf desarrollaron por primera vez la suite de protocolos TCP/IP que incluía IPv4 en 1981, nunca imaginaron en qué podría llegar a convertirse Internet. En aquel entonces, la computadora personal era, en la mayoría de los casos, una curiosidad para los aficionados, y todavía faltaba más de una década para la aparición de la World Wide Web.

Con la proliferación de los dispositivos informáticos personales y la llegada de la World Wide Web, pronto resultó evidente que las 4300 millones de direcciones IPv4 no serían suficientes. La solución a largo plazo era el protocolo IPv6, pero se necesitaban soluciones más inmediatas para abordar el agotamiento. A corto plazo, el IETF implementó varias soluciones, entre las que se incluía la traducción de direcciones de red (NAT) y las direcciones IPv4 privadas definidas en RFC 1918. En este capítulo, se analiza cómo se utiliza NAT combinada con el espacio de direcciones privadas para conservar y usar de forma más eficaz las direcciones IPv4, a fin de proporcionar acceso a Internet para las redes de todos los tamaños. En este capítulo, se abarcan los siguientes temas:

* Las características, la terminología y las operaciones generales de NAT
* Los diferentes tipos de NAT, incluidas la NAT estática, la NAT dinámica y la NAT con sobrecarga
* Las ventajas y las desventajas de NAT
* La configuración, la verificación y el análisis de la NAT estática, la NAT dinámica y la NAT con sobrecarga
* La forma en que se puede usar el reenvío de puertos para acceder a los dispositivos internos desde Internet
* La resolución de problemas de NAT mediante los comandos **show** y**debug**
* La forma en que se utiliza NAT para IPv6 para traducir entre direcciones IPv6 y direcciones IPv4





## Funcionamiento de NAT

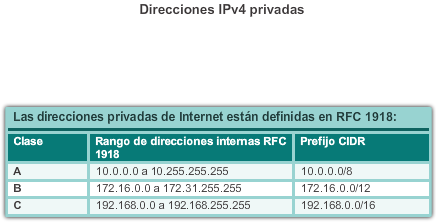
### Características de NAT

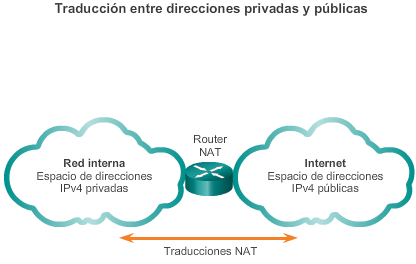
No existen suficientes direcciones IPv4 públicas para asignar una dirección única a cada dispositivo conectado a Internet. Las redes suelen implementarse mediante el uso de direcciones IPv4 privadas, según se definen en RFC 1918. En la figura 1, se muestra el rango de direcciones incluidas en RFC 1918. Es muy probable que la computadora que utiliza para ver este curso tenga asignada una dirección privada.

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.

Como se muestra en la figura 2, 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, las cuales se analizan más adelante en este capítulo. La solución al agotamiento del espacio de direcciones IPv4 y a las limitaciones de NAT es la transición final a IPv6.





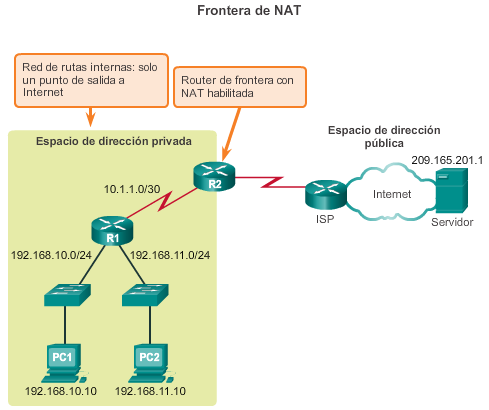
NAT tiene muchos usos, pero el principal es conservar las direcciones IPv4 públicas. Esto se logra al permitir que las redes utilicen direcciones IPv4 privadas internamente y al proporcionar la traducción a una dirección pública solo cuando sea necesario. NAT tiene el beneficio adicional de proporcionar 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. En el ejemplo de la ilustración, el R2 es un router de frontera. Visto desde el ISP, el R2 forma una red de rutas internas.

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.

**Nota:** la conexión al ISP también puede utilizar una dirección privada o pública compartida entre clientes. A los fines de este capítulo, se muestra una dirección pública.



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.

NAT incluye cuatro tipos de direcciones:

* Dirección local interna
* Dirección global interna
* Dirección local externa
* Dirección global externa

Al determinar qué tipo de dirección se utiliza, es importante recordar que la terminología de NAT siempre se aplica desde la perspectiva del dispositivo con la dirección traducida:

* **Dirección interna:** la dirección del dispositivo que se traduce por medio de NAT.
* **Dirección externa:** la dirección del dispositivo de destino.

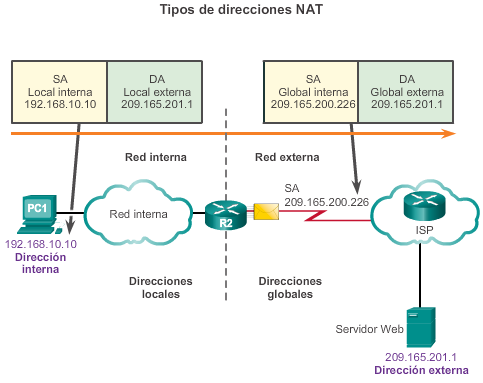
NAT también usa los conceptos de local o global con relación a las direcciones:

* **Dirección local:** cualquier dirección que aparece en la porción interna de la red.
* **Dirección global:** cualquier dirección que aparece en la porción externa de la red.

En la ilustración, la PC1 tiene la dirección local interna 192.168.10.10. Desde la perspectiva de la PC1, el servidor web tiene la dirección externa 209.165.201.1. Cuando se envían los paquetes de la PC1 a la dirección global del servidor web, la dirección local interna de la 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.

Observe que la 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 la 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.

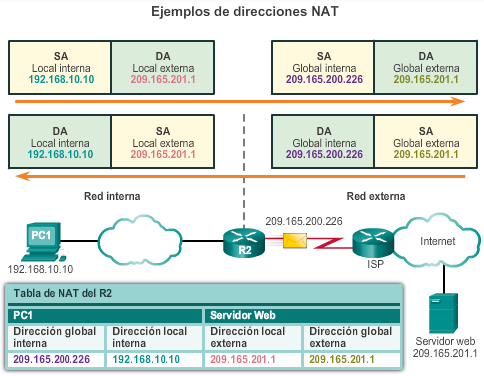


Los términos “interna” y “externa” se combinan con los términos “global” y “local” para hacer referencia a direcciones específicas. En la ilustración, el router R2 se configuró para proporcionar NAT. Este tiene un conjunto de direcciones públicas para asignar a los hosts internos.

* **Dirección local interna:** la dirección de origen vista desde el interior de la red. En la ilustración, la dirección IPv4 192.168.10.10 se asignó a la PC1. Esta es la dirección local interna de la PC1.
* **Dirección global interna:** la dirección de origen vista desde la red externa. En la ilustración, cuando se envía el tráfico de la PC1 al servidor web en 209.165.201.1, el R2 traduce la dirección local interna a una dirección global interna. En este caso, el R2 cambia la dirección IPv4 de origen de 192.168.10.10 a 209.165.200.226. De acuerdo con la terminología de NAT, la dirección local interna 192.168.10.10 se traduce a la dirección global interna 209.165.200.226.
* **Dirección global externa:** la dirección del destino vista desde la red externa. Es una dirección IPv4 enrutable globalmente y asignada a un host en Internet. Por ejemplo, se puede llegar al servidor web en la dirección IPv4 209.165.201.1. Por lo general, las direcciones externas globales y locales son iguales.
* **Dirección local externa:** la dirección del destino vista desde la red interna. En este ejemplo, 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.

En la ilustración, se muestra cómo se dirige el tráfico que se envía desde una computadora interna hacia un servidor web externo a través del router con NAT habilitada. También se muestra cómo se dirige y se traduce inicialmente el tráfico de retorno.

**Nota:** el uso de la dirección local externa excede el ámbito de este curso.



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

Haga clic en el botón Reproducir de la figura para iniciar la animación.

La PC1 envía un paquete dirigido al servidor web. El R1 reenvía el paquete al R2.

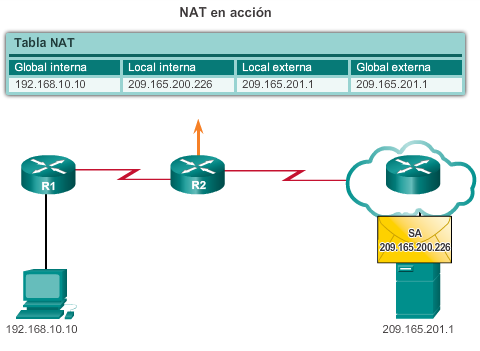
Cuando el paquete llega al R2, el router con NAT habilitada para la red, el R2 lee la dirección IPv4 de destino del paquete para determinar si este cumple con los criterios especificados para la traducción.

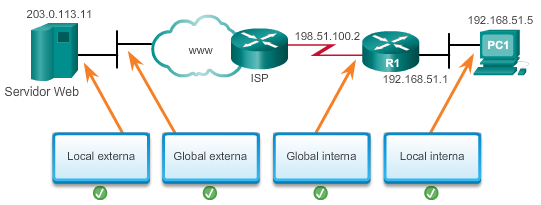
En este caso, la dirección IPv4 de origen cumple con los criterios y se traduce de 192.168.10.10 (dirección local interna) a 209.165.200.226 (dirección global interna). El R2 agrega esta asignación de dirección local a global a la tabla de NAT.

El R2 envía el paquete con la dirección de origen traducida hacia el destino.

El servidor web responde con un paquete dirigido a la dirección global interna de la PC1 (209.165.200.226).

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.





### 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).

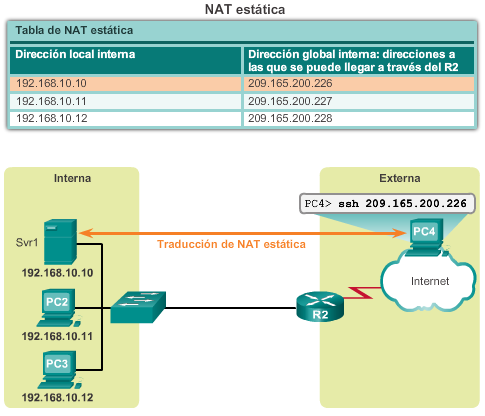
**NAT estática**

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, la PC2 y la 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.

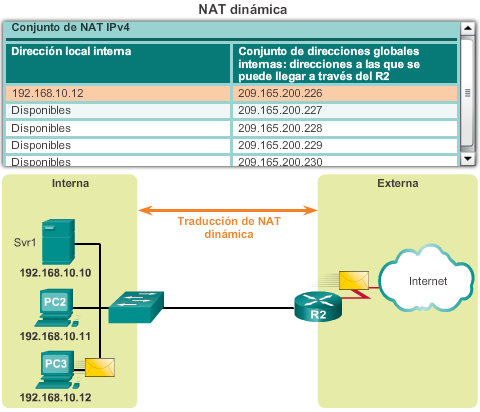
La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener una dirección constante que sea accesible tanto desde Internet, como desde el servidor web de una empresa. También es útil para los dispositivos a los que debe poder acceder el personal autorizado cuando 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.

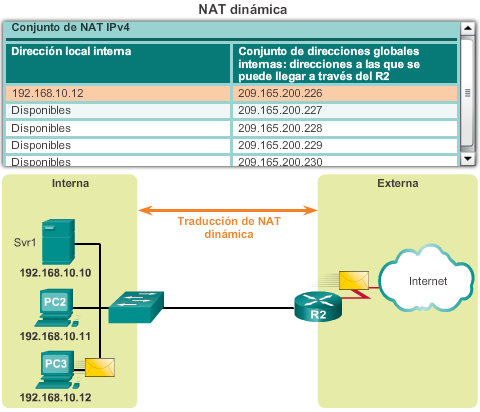
La NAT estática requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.



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.





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.

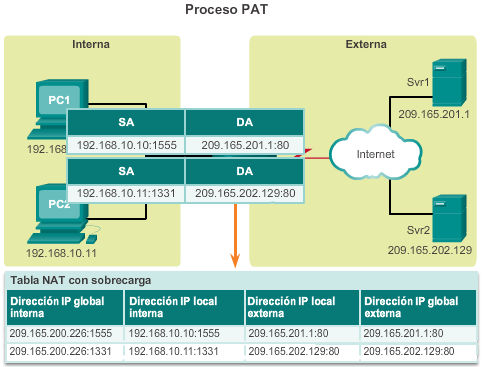
PAT garantiza que los dispositivos usen un número de puerto TCP distinto para cada sesión con un servidor en Internet. Cuando llega una respuesta del servidor, el número de puerto de origen, que se convierte en el número de puerto de destino en la devolución, determina a qué dispositivo el router reenvía 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.

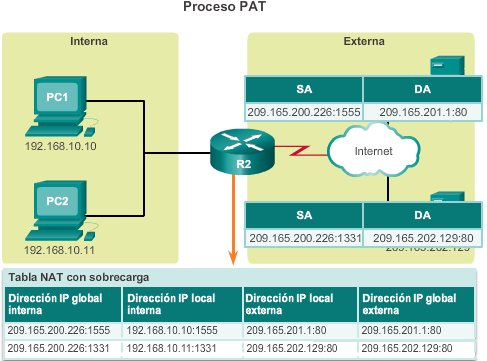
Haga clic en los botones Reproducir y Pausa de la ilustración para controlar la animación.

En la animación, se muestra el proceso de PAT. PAT agrega números de puerto de origen únicos a la dirección global interna para distinguir las traducciones.

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: HTTP.

Para la dirección de origen, el R2 traduce la dirección local interna a una dirección global interna con el número de puerto agregado. La dirección de destino no se modifica, pero ahora se la denomina “dirección IP global externa”. Cuando el servidor web responde, se invierte la ruta.



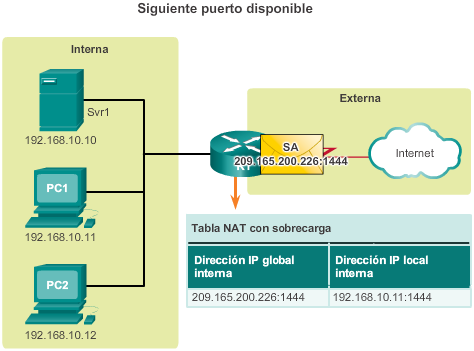


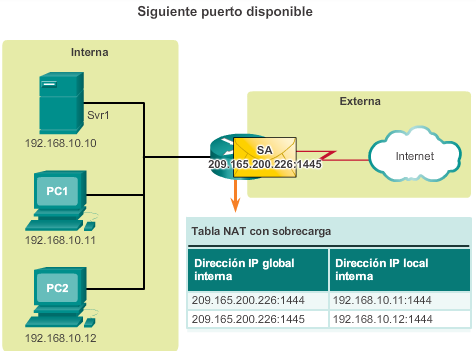
En el ejemplo anterior, los números de puerto del cliente, 1331 y 1555, no se modificaron en el router con NAT habilitada. Esta no es una situación muy probable, porque existe una gran posibilidad de que estos números de puerto ya se hayan conectado a otras sesiones activas.

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.

Haga clic en el botón Reproducir de la ilustración para ver el funcionamiento de PAT.

En la animación, 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.





Hacer un resumen de las diferencias entre NAT y PAT contribuye a la comprensión de ambas.

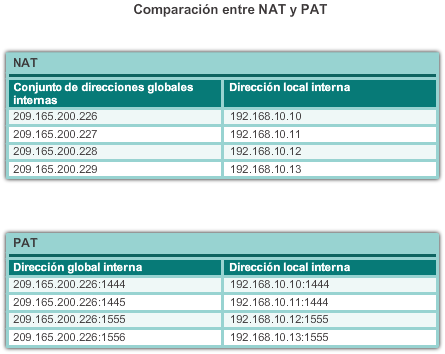
Como se muestran en la ilustración, NAT traduce direcciones IPv4 en una relación de 1:1 entre direcciones IPv4 privadas y direcciones IPv4 públicas. Sin embargo, PAT modifica la dirección y el número de puerto.

NAT reenvía los paquetes entrantes a su destino interno mediante la dirección IPv4 de origen de entrada proporcionada por el host en la red pública. En general, con PAT hay solo una o muy pocas direcciones IPv4 públicamente expuestas. Los paquetes entrantes de la red pública se enrutan a sus destinos en la red privada consultando una tabla en el router NAT. Esta tabla hace un seguimiento de los pares de puertos públicos y privados. Esto se denomina “seguimiento de conexiones”.

**Paquetes sin segmento de capa 4**

¿Qué sucede con los paquetes IPv4 que transportan datos que no son segmentos TCP o UDP? Estos paquetes no contienen un número de puerto de capa 4. PAT traduce la mayoría de los protocolos comunes transmitidos mediante IPv4 que no utilizan TCP o UDP como protocolo de la capa de transporte. El más común de ellos es ICMPv4. PAT maneja cada uno de estos tipos de protocolos de manera diferente. Por ejemplo, los mensajes de consulta, las solicitudes de eco y las respuestas de eco de ICMPv4 incluyen una ID de consulta. ICMPv4 utiliza la ID de consulta para identificar una solicitud de eco con su respectiva respuesta. La ID de consulta aumenta con cada solicitud de eco enviada. PAT utiliza la ID de consulta en lugar de un número de puerto de capa 4.

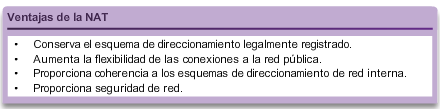
**Nota:** otros mensajes ICMPv4 no utilizan la ID de consulta. Estos mensajes y otros protocolos que no utilizan los números de puerto TCP o UDP varían y exceden el ámbito de este currículo.



### Beneficios de NAT

NAT ofrece varios beneficios, incluidos los siguientes:

* NAT conserva el esquema de direccionamiento legalmente registrado al permitir la privatización de las intranets. NAT conserva las direcciones mediante la multiplexación de aplicaciones en el nivel de puerto. Con la NAT con sobrecarga, los hosts internos pueden compartir una única dirección IPv4 pública para todas las comunicaciones externas. En este tipo de configuración, se requieren muy pocas direcciones externas para admitir varios hosts internos.
* NAT aumenta la flexibilidad de las conexiones a la red pública. Se pueden implementar varios conjuntos y conjuntos de respaldo y de equilibrio de carga para asegurar conexiones de red pública confiables.
* NAT proporciona coherencia a los esquemas de direccionamiento de red interna. Para cambiar el esquema de direcciones IPv4 públicas en una red que no utiliza direcciones IPv4 privadas ni NAT, se requiere redireccionar todos los hosts en la red existente. Los costos de redireccionamiento de hosts pueden ser considerables. NAT permite mantener el esquema de direcciones IPv4 privadas existente a la vez que facilita el cambio a un nuevo esquema de direccionamiento público. Esto significa que una organización podría cambiar los ISP sin necesidad de modificar ninguno de sus clientes internos.
* NAT proporciona seguridad de red. Debido a que las redes privadas no anuncian sus direcciones ni su topología interna, son razonablemente seguras cuando se utilizan en conjunto con NAT para obtener acceso externo controlado. Sin embargo, NAT no reemplaza a los firewalls.



NAT presenta algunas desventajas. El hecho de que los hosts en Internet parezcan comunicarse de forma directa con el dispositivo con NAT habilitada, en lugar de hacerlo con el host real dentro de la red privada, genera una serie de inconvenientes.

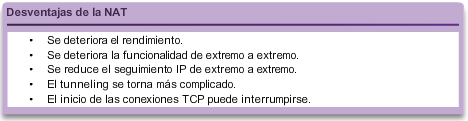
Una desventaja del uso de NAT se relaciona con el rendimiento de la red, en especial, en el caso de los protocolos en tiempo real como VoIP. NAT aumenta los retrasos de switching porque la traducción de cada dirección IPv4 dentro de los encabezados del paquete lleva tiempo. Al primer paquete se aplica el switching de procesos; esto siempre se realiza 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 demoran.

Otra desventaja del uso de NAT es que 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. Por ejemplo, algunas aplicaciones de seguridad, como las firmas digitales, fallan porque la dirección IPv4 de origen cambia antes de llegar a destino. Las aplicaciones que utilizan direcciones físicas, en lugar de un nombre de dominio calificado, no llegan a los destinos que se traducen a través del router NAT. En ocasiones, este problema se puede evitar al implementar las asignaciones de NAT estática.

También se reduce el seguimiento IPv4 de extremo a extremo. El seguimiento de los paquetes que pasan por varios cambios de dirección a través de varios saltos de NAT se torna mucho más difícil y, en consecuencia, dificulta la resolución de problemas.

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.

Los servicios que requieren que se inicie una conexión TCP desde la red externa, o “protocolos sin estado”, como los servicios que utilizan UDP, pueden interrumpirse. A menos que el router NAT esté configurado para admitir dichos protocolos, los paquetes entrantes no pueden llegar a su destino. Algunos protocolos pueden admitir una instancia de NAT entre los hosts participantes (por ejemplo, FTP de modo pasivo), pero fallan cuando NAT separa a ambos sistemas de Internet.



## Configuración de 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 la figura 1, 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.

Existen dos pasos básicos para configurar las traducciones NAT estáticas.

**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.

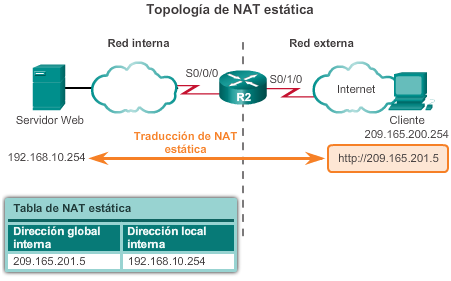
**Paso 2.** Una vez configurada la asignación, las interfaces que participan en la traducción se configuran como interna o externa con respecto a NAT. En el ejemplo, la interfaz Serial 0/0/0 del R2 es una interfaz interna, y la interfaz Serial 0/1/0 es una interfaz externa.

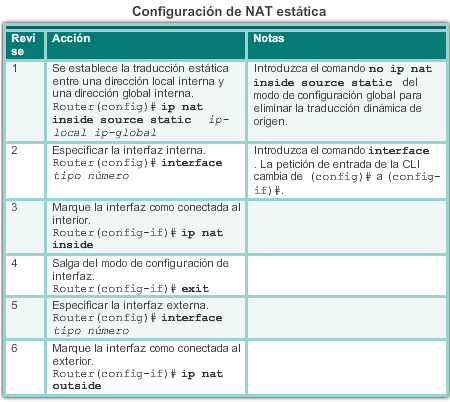
Los paquetes que llegan hasta la interfaz interna del R2 (Serial 0/0/0) desde la dirección IPv4 local interna configurada (192.168.10.254) se traducen y, luego, se reenvían hacia la red externa. Los paquetes que llegan a la interfaz externa del R2 (Serial 0/1/0), que están dirigidos a la dirección IPv4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

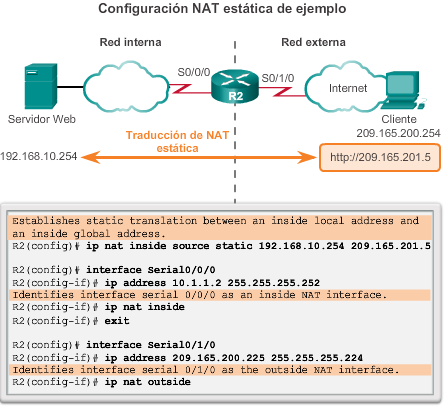
En la figura 2, se describen los comandos necesarios para configurar la NAT estática.

En la figura 3, se muestran los comandos necesarios en el R2 para crear una asignación de NAT estática al servidor web en la topología de ejemplo. 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.

Utilice el verificador de sintaxis de la figura 4 para configurar una entrada de NAT estática adicional en el R2.







Con la configuración anterior, en la ilustración se muestra el proceso de traducción de NAT estática entre el cliente y el servidor web. En general, las traducciones estáticas se utilizan cuando los clientes en la red externa (Internet) necesitan llegar a los servidores en la red interna.

1. El cliente desea establecer una conexión al servidor web. El cliente envía un paquete al servidor web con la dirección IPv4 pública de destino 209.165.201.5. Esta es la dirección global interna del servidor web.

2. El primer paquete que recibe del cliente en su interfaz NAT externa ocasiona que el R2 revise su tabla de NAT. Una vez que se encuentra la dirección IPv4 de destino en la tabla de NAT, se traduce.

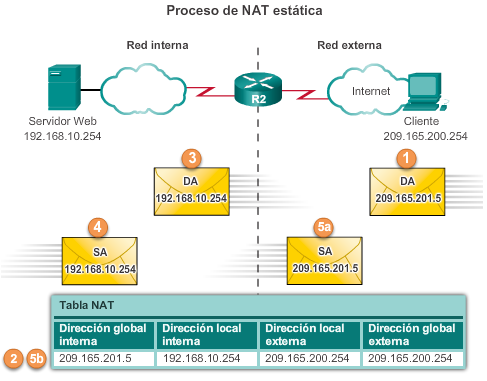
3. El R2 reemplaza la dirección global interna 209.165.201.5 por la dirección local interna 192.168.10.254. Luego, el R2 reenvía el paquete hacia el servidor web.

4. El servidor web recibe el paquete y responde al cliente con la dirección local interna, 192.168.10.254.

5a. El R2 recibe el paquete del servidor web en su interfaz NAT interna con la dirección de origen de la dirección local interna del servidor web, 192.168.10.254.

5b. El R2 busca una traducción para la dirección local interna en la tabla de NAT. La dirección se encuentra en esa tabla. El R2 traduce la dirección de origen a la dirección global interna 209.165.201.5 y reenvía el paquete por su interfaz serial 0/1/0 hacia el cliente.

6. El cliente recibe el paquete y continúa la conversación. El router NAT lleva a cabo los pasos 2 a 5b para cada paquete. (El paso 6 no aparece en la ilustración).

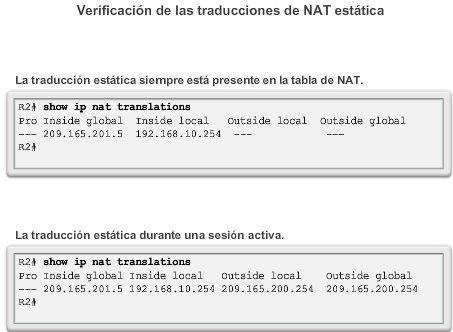


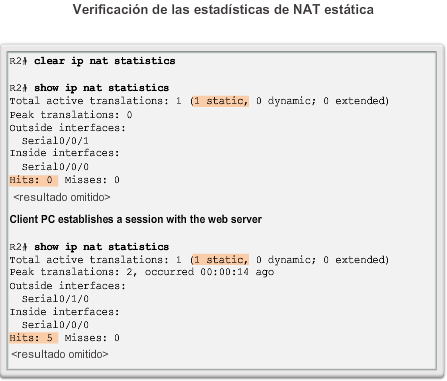
El comando **show ip nat translations** es útil para verificar el funcionamiento de NAT. Este comando muestra las traducciones NAT activas. A diferencia de las traducciones dinámicas, las traducciones estáticas siempre figuran en la tabla de NAT. En la figura 1, se muestra el resultado de este comando con el ejemplo de configuración anterior. 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. Si se emite el comando durante una sesión activa, el resultado también indica la dirección del dispositivo externo, como se muestra en la figura 1.

Otro comando útil es **show ip nat statistics**. Como se muestra en la figura 2, el comando **show ip nat statistics** muestra información sobre la cantidad total de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad de direcciones que se asignaron.

Para verificar que la traducción NAT funcione, es conveniente borrar las estadísticas de todas las traducciones anteriores con el comando **clear ip nat statistics** antes de realizar la prueba.

Antes de cualquier comunicación con el servidor web, el comando **show ip nat statistics** no muestra ningún acierto actual. Una vez que el cliente establece una sesión con el servidor web, el comando **show ip nat statistics** muestra cinco aciertos. De este modo, se verifica que se lleva a cabo la traducción de NAT estática en el R2.





### Configuración de NAT dinámica

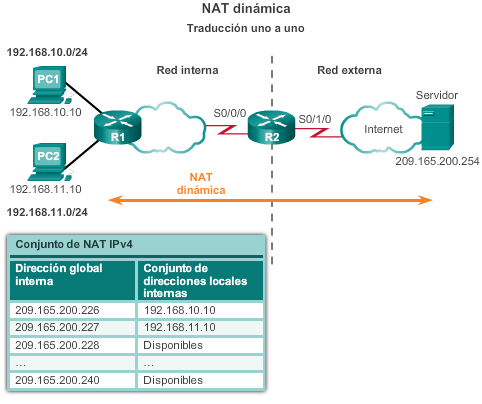
Mientras que la NAT estática proporciona una asignación permanente entre una dirección local interna y una dirección global interna, la NAT dinámica permite la asignación automática de direcciones locales internas a direcciones globales internas. Por lo general, estas direcciones globales internas son 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.

**Nota:** la traducción entre direcciones IPv4 públicas y privadas es el uso más frecuente de NAT. No obstante, las traducciones de NAT se pueden realizar entre cualquier par 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.

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.



En la figura 1, se muestran los pasos y los comandos utilizados para configurar la NAT dinámica.

**Paso 1.**Defina 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.

**Paso 2.**Configure una ACL estándar para identificar (permitir) solo aquellas direcciones que se deben traducir. Una ACL demasiado permisiva puede generar resultados impredecibles. Recuerde que al final de cada ACL hay una instrucción implícita para **denegar todo**.

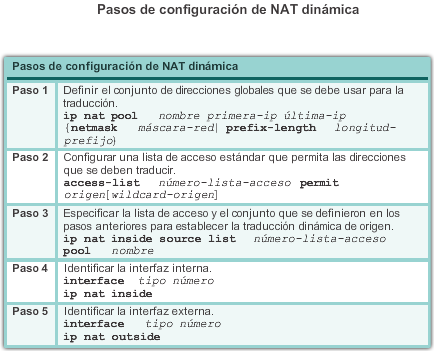
**Paso 3.**Conecte la ACL al conjunto. Para conectar la ACL al conjunto, se utiliza el comando **ip nat inside source list***número-lista-acceso***number pool***nombre-conjunto*. El router utiliza esta configuración para determinar qué dirección (**pool**) recibe cada dispositivo (**list**).

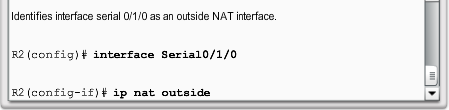
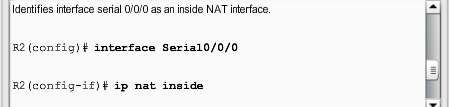
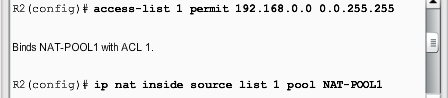
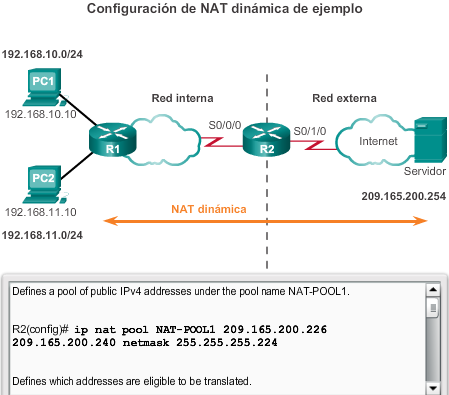
**Paso 4.**Identifique qué interfaces son internas con respecto a NAT; es decir, cualquier interfaz que se conecte a la red interna.

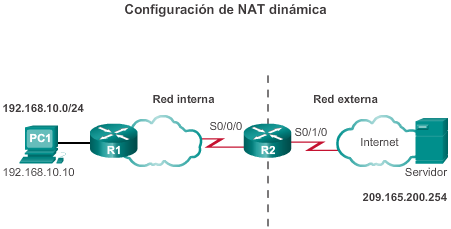
**Paso 5.** Identifique qué interfaces son externas con respecto a NAT; es decir, cualquier interfaz que se conecte a la red externa.

En la figura 2, se muestra una topología y una configuración de ejemplo. Esta configuración permite la traducción para todos los hosts en la red 192.168.0.0/16, que incluye las LAN 192.168.10.0 y 192.168.11.0, cuando generan tráfico que ingresa por S0/0/0 y sale por S0/1/0. Estos hosts se traducen a una dirección disponible del conjunto en el rango de 209.165.200.226 a 209.165.200.240.

En la figura 3, se muestra la topología utilizada para la configuración del verificador de sintaxis. Utilice el verificador de sintaxis de la figura 4 para configurar la NAT dinámica en el R2.







Con la configuración anterior, en las ilustraciones se muestra el proceso de traducción de NAT dinámica entre dos clientes y el servidor web:

En la figura 1, se muestra el flujo de tráfico desde adentro hacia fuera:

1. Los hosts con las direcciones IPv4 de origen (192.168.10.10 [PC1] y 192.168.11.10 [PC2]) envían paquetes para solicitar la conexión al servidor en la dirección IPv4 pública (209.165.200.254).

2. El R2 recibe el primer paquete del host 192.168.10.10. Debido a que este paquete se recibió en una interfaz configurada como interfaz NAT interna, el R2 verifica la configuración NAT para determinar si este paquete debe traducirse. Como la ACL permite este paquete, el R2 lo traduce. El R2 consulta su tabla de NAT. Debido a que no hay entrada de traducción para esta dirección IP, el R2 determina que la dirección de origen 192.168.10.10 se debe traducir de manera dinámica. El R2 selecciona una dirección global disponible del conjunto de direcciones dinámicas y crea una entrada de traducción, 209.165.200.226. La dirección IPv4 de origen inicial (192.168.10.10) es la dirección local interna, y la dirección traducida es la dirección global interna (209.165.200.226) en la tabla de NAT.

Para el segundo host, 192.168.11.10, el R2 repite el procedimiento, selecciona la siguiente dirección global disponible del conjunto de direcciones dinámicas y crea una segunda entrada de traducción, 209.165.200.227.

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 se lleva a cabo para el paquete de la PC2 con la dirección traducida para esta computadora (209.165.200.227).

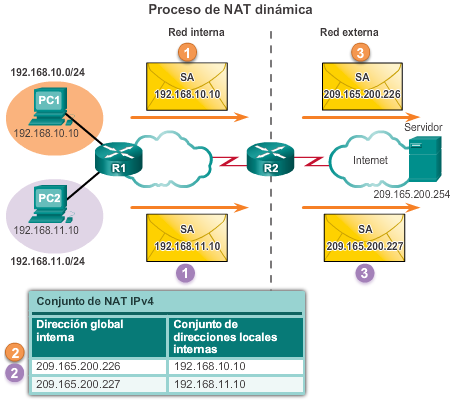
En la figura 2, se muestra el flujo de tráfico desde adentro hacia fuera:

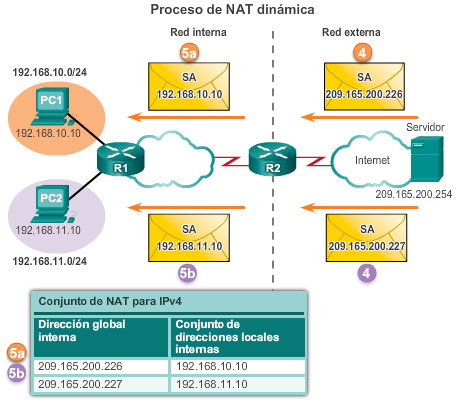
4. El servidor recibe el paquete de la PC1 y responde con la dirección IPv4 de destino 209.165.200.226. Cuando el servidor recibe el segundo paquete, responde a la PC2 con la dirección IPv4 de destino 209.165.200.227.

5a. Cuando el R2 recibe el paquete con la dirección IPv4 de destino 209.165.200.226, realiza una búsqueda en la tabla de NAT. Con la asignación de la tabla, el R2 vuelve a traducir la dirección a la dirección local interna (192.168.10.10) y reenvía el paquete hacia la PC1.

5b. Cuando el R2 recibe el paquete con la dirección IPv4 de destino 209.165.200.227, realiza una búsqueda en la tabla de NAT. Con la asignación de la tabla, el R2 vuelve a traducir la dirección a la dirección local interna (192.168.11.10) y reenvía el paquete hacia la PC2.

6. La PC1 en 192.168.10.10 y la PC2 en 192.168.11.10 reciben los paquetes y continúan la conversación. El router lleva a cabo los pasos 2 a 5 para cada paquete. (El paso 6 no aparece en las ilustraciones).





El resultado del comando **show ip nat translations** que aparece en la figura 1 muestra los detalles de las dos asignaciones de NAT anteriores. El comando muestra todas las traducciones estáticas que se configuraron y todas las traducciones dinámicas que se crearon a causa del tráfico.

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.

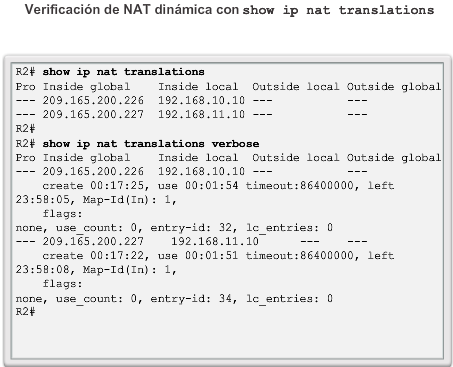
De manera predeterminada, a las entradas de traducción se les agota el tiempo de espera después de 24 horas, a menos que se vuelvan a configurar los temporizadores con el comando **ip nat translation timeout***segundos-tiempo-espera*en el modo de configuración global.

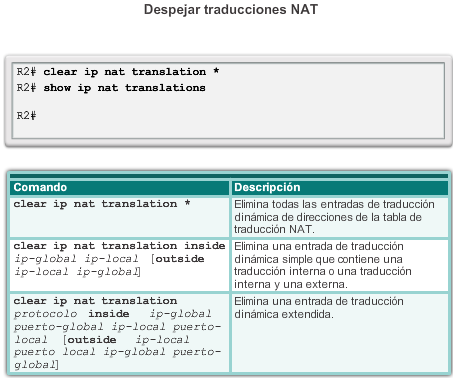
Para borrar las entradas dinámicas antes de que se agote el tiempo de espera, utilice el comando **clear ip nat translation** en el modo de configuración global (figura 2). Es útil borrar las entradas dinámicas al probar la configuración NAT. Como se muestra en la tabla, este comando se puede utilizar con palabras clave y variables para controlar qué entradas se deben borrar. Se pueden borrar entradas específicas para evitar interrumpir las sesiones activas. Utilice el comando de configuración global **clear ip nat translation \*** para borrar todas las traducciones de la tabla.

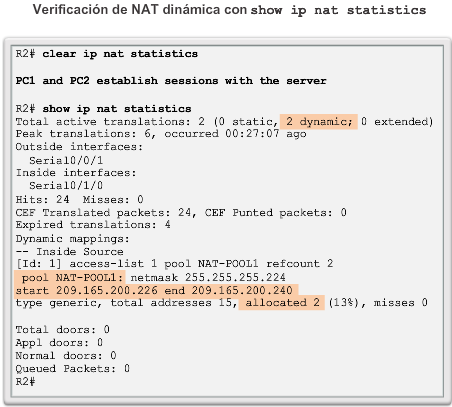
**Nota:** solo se borran de la tabla las traducciones dinámicas. Las traducciones estáticas no pueden borrarse de la tabla de traducción.

En la figura 3, el comando **show ip nat statistics** muestra la información sobre la cantidad total de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad de direcciones que se asignaron.

También puede utilizar el comando **show running-config** y buscar los comandos de NAT, ACL, interfaz o conjunto con los valores requeridos. Examínelos detenidamente y corrija cualquier error que detecte.







### Configuración de la traducción de la dirección del puerto (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. En otras palabras, se puede utilizar una única dirección IPv4 pública para cientos, incluso miles de direcciones IPv4 privadas internas. Cuando se configura este tipo de traducción, el router mantiene suficiente información acerca de los protocolos de nivel superior, de los números de puerto 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.

**Nota:** la cantidad total de direcciones internas que se pueden traducir a una dirección externa teóricamente podría ser de hasta 65 536 por dirección IP. Sin embargo, la cantidad de direcciones internas a las que se puede asignar una única dirección IP es aproximadamente 4000.

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.

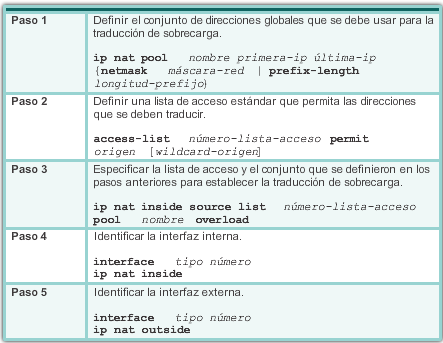
**Configuración de PAT para un conjunto de direcciones IP públicas**

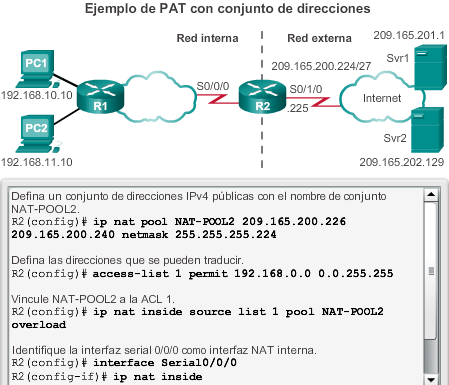
Si se emitió más de una dirección IPv4 pública para un sitio, estas direcciones pueden ser parte de un conjunto utilizado por PAT. Esto es similar a la NAT dinámica, con la excepción de que no existen suficientes direcciones públicas para realizar una asignación uno a uno entre direcciones internas y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

En la figura 1, 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 en la figura 2 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.

Utilice el verificador de sintaxis de la figura 3 para configurar PAT con un conjunto de direcciones en el R2.





**Configuración de PAT para una única dirección IPv4 pública**

En la figura 1, se muestra la topología de una implementación de PAT para la traducción de 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**.

En la figura 2, se muestran los pasos que se deben seguir para configurar PAT con una única dirección IPv4. 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.** Defina una ACL para permitir que se traduzca el tráfico.

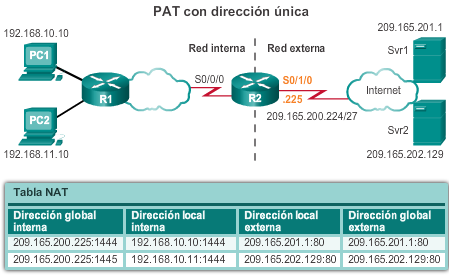
**Paso 2.**Configure la traducción de origen con las palabras clave **interface** y**overload**. La palabra clave **interface** identifica la dirección IP de la interfaz que se debe utilizar en la traducción de las direcciones internas. La palabra clave **overload** le indica al router que realice un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

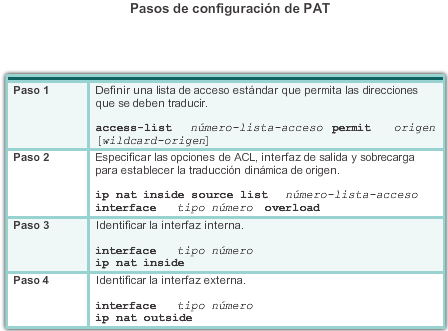
**Paso 3.**Identifique cuáles son las interfaces internas con respecto a NAT. Es decir, toda interfaz que se conecte a la red interna.

**Paso 4.**Identifique 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.

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.

Utilice el verificador de sintaxis de la figura 3 para configurar PAT con una única dirección en el R2.





El proceso de NAT con sobrecarga es el mismo, ya sea que se utilice un conjunto de direcciones o una única dirección. En el ejemplo anterior de PAT, la PC1 desea comunicarse con el servidor web Svr1 por medio de una única dirección IPv4 pública. Al mismo tiempo, otro cliente, la PC2, desea establecer una sesión similar con el servidor web Svr2. Tanto la PC1 como la PC2 se configuraron con direcciones IPv4 privadas, con el R2 habilitado para PAT.

**Proceso de la computadora al servidor**

1. En la figura 1, se muestra que la PC1 y la PC2 envían paquetes a los servidores Svr1 y Svr2, respectivamente. La PC1 tiene la dirección IPv4 de origen 192.168.10.10 y utiliza el puerto de origen TCP 1444. La PC2 tiene la dirección IPv4 de origen 192.168.10.11 y, por casualidad, se le asigna el mismo puerto de origen 1444.

2. El paquete de la PC1 llega primero al R2. Mediante el uso de PAT, el R2 modifica la dirección IPv4 de origen a 209.165.200.225 (dirección global interna). En la tabla de NAT, no hay ningún otro dispositivo que use el puerto 1444, de modo que PAT mantiene el mismo número de puerto. El paquete luego se reenvía hacia el Svr1 en 209.165.201.1.

3. A continuación, llega el paquete de la PC2 al R2. PAT está configurada para utilizar una única dirección IPv4 global interna para todas las traducciones, 209.165.200.225. Al igual que con el proceso de traducción para la PC1, PAT cambia la dirección IPv4 de origen de la PC2 a la dirección global interna 209.165.200.225. Sin embargo, la PC2 tiene el mismo número de puerto de origen que una entrada actual de PAT, la traducción para la PC1. PAT aumenta el número de puerto de origen hasta que sea un valor único en su tabla. En este caso, la entrada del puerto de origen en la tabla de NAT y el paquete de la PC2 reciben el número 1445.

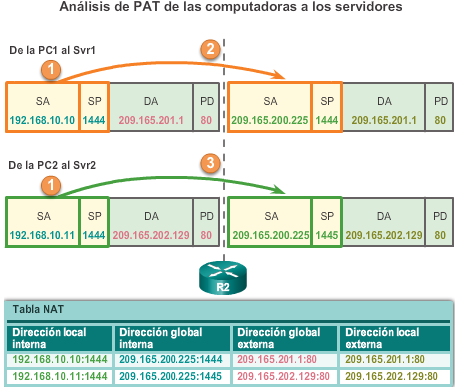
Si bien la PC1 y la PC2 usan la misma dirección traducida, la dirección global interna 209.165.200.225, y el mismo número de puerto de origen 1444, el número de puerto modificado para la PC2 (1445) hace que cada entrada en la tabla de NAT sea única. Esto se torna evidente cuando los paquetes se devuelven desde los servidores hacia los clientes.

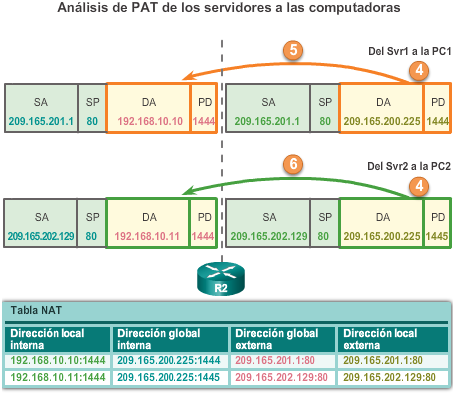
**Proceso del servidor a la computadora**

4. Como se muestra en la figura 2, en un intercambio típico entre cliente y servidor, los servidores Svr1 y Svr2 responden a las solicitudes recibidas de la PC1 y la PC2, respectivamente. 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. Al parecer, los servidores se comunican con el mismo host en 209.165.200.225, pero no es así.

5. A medida que llegan los paquetes, el R2 ubica una única entrada en su tabla de NAT mediante la dirección de destino y el puerto de destino de cada paquete. En el caso del paquete del Svr1, la dirección IPv4 de destino 209.165.200.225 tiene varias entradas, pero solo una con el puerto de destino 1444. Mediante la entrada de su tabla, el R2 cambia la dirección IPv4 de destino del paquete a 192.168.10.10, sin necesidad de modificar el puerto de destino. Luego, el paquete se reenvía hacia la PC1.

6. Cuando llega el paquete del Svr2, el R2 realiza una traducción similar. La dirección IPv4 de destino 209.165.200.225 vuelve a aparecer en varias entradas. Sin embargo, con el puerto de destino 1445, el R2 puede identificar una única entrada de traducción. La dirección IPv4 de destino se modifica a 192.168.10.11. En este caso, el puerto de destino también se debe volver a modificar a su valor original de 1444, que está almacenado en la tabla de NAT. Luego, el paquete se reenvía hacia la PC2.

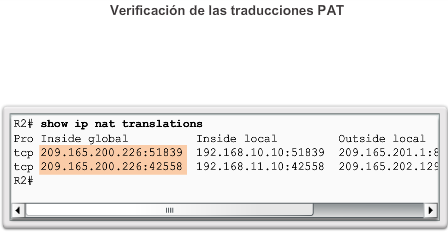


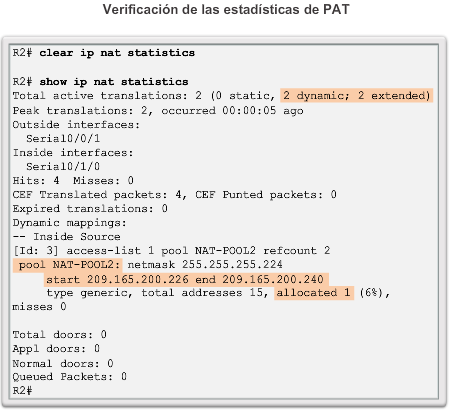


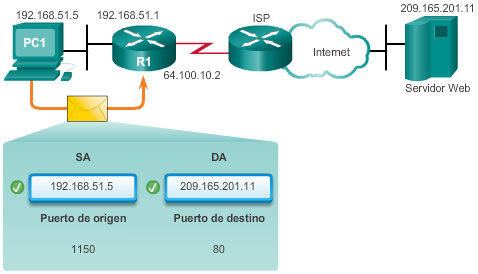
El router R2 se configuró para proporcionar PAT a los clientes de 192.168.0.0/16. Cuando los hosts internos salen del router R2 a Internet, se traducen a una dirección IPv4 del conjunto de PAT con un único número de puerto de origen.

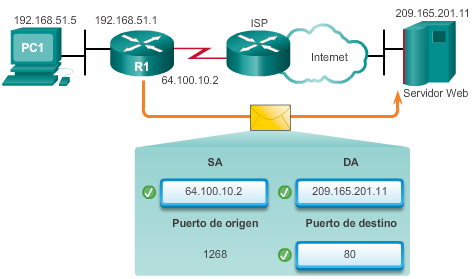
Para verificar PAT, se usan los mismos comandos que se usan para verificar la NAT estática y dinámica, como se muestra en la figura 1. El comando **show ip nat translations** muestra las traducciones de dos hosts distintos a servidores web distintos. Observe que se asigna la misma dirección IPv4 209.165.200.226 (dirección global interna) a dos hosts internos distintos. Los números de puerto de origen en la tabla de NAT distinguen las dos transacciones.

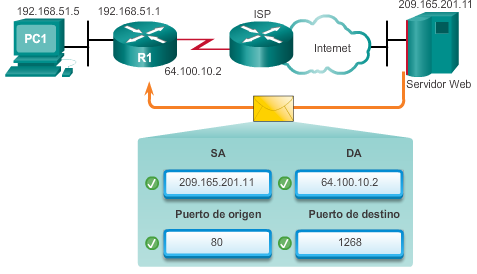
Como se muestra en la figura 2, el comando **show ip nat statistics** verifica que NAT-POOL2 haya asignado una única dirección para ambas traducciones. El resultado incluye información sobre la cantidad y el tipo de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad que se asignó.

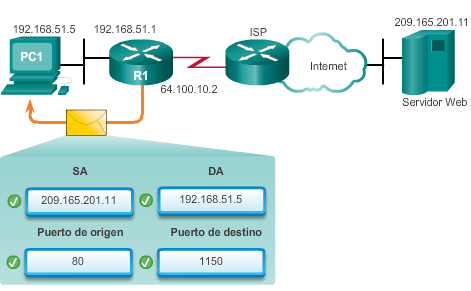












### Reenvío de puertos

El reenvío de puertos (a veces, denominado “tunneling”) consiste en reenviar un puerto de red 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 del router se reenvíen o se abran para permitir que estas aplicaciones funcionen, como se muestra en la figura 1. 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.

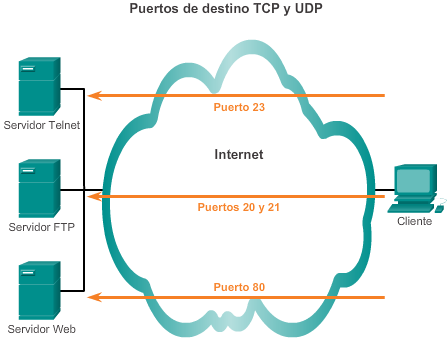
El problema es que NAT no permite las solicitudes iniciadas desde el exterior. Esta situación se puede resolver de forma manual. El reenvío de puertos se puede configurar para identificar los puertos específicos que se pueden reenviar a los hosts internos.

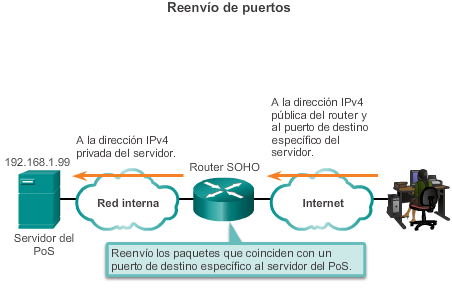
Recuerde que las aplicaciones de software de Internet interactúan con los puertos de usuario que necesitan estar abiertos o disponibles para dichas aplicaciones. Las distintas aplicaciones usan puertos diferentes. Esto hace que las aplicaciones y los routers identifiquen los servicios de red de manera predecible. Por ejemplo, HTTP funciona a través del puerto bien conocido 80. Cuando alguien introduce la dirección **http://cisco.com**, el explorador muestra el sitio web de Cisco Systems, Inc. Tenga 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.

En la figura 2, se muestra al propietario de una pequeña empresa que utiliza un servidor del punto de venta (PoS) para hacer un seguimiento de las ventas y los inventarios en la tienda. Se puede acceder al servidor desde la tienda pero, debido a que tiene una dirección IPv4 privada, no es posible acceder a este de manera pública desde Internet. Habilitar el router local para el reenvío de puertos permitiría que el propietario acceda al servidor del punto de venta en cualquier lugar desde Internet. El reenvío de puertos en el router se configura con el número de puerto de destino y la dirección IPv4 privada del servidor del punto de venta. Para acceder al servidor, el software de cliente utilizaría la dirección IPv4 pública del router y el puerto de destino del servidor.



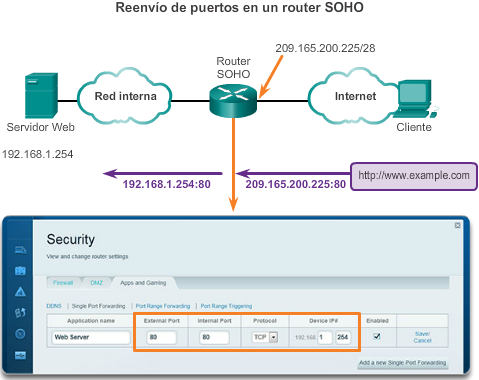


En la ilustración, se muestra la ventana de configuración Single Port Forwarding (Reenvío de puerto único) de un router SOHO Linksys EA6500. De manera predeterminada, el reenvío de puertos no está habilitado en el router.

Si se especifica la dirección local interna a la cual se deben reenviar las solicitudes, es posible habilitar el reenvío de puertos para las aplicaciones. En la ilustración, las solicitudes de servicio HTTP que llegan a este router Linksys se reenvían al servidor web con la dirección local interna 192.168.1.254. Si la dirección IPv4 WAN externa del router SOHO es 209.165.200.225, el usuario externo puede introducir **http://www.ejemplo.com**, y el router Linksys redirige la solicitud HTTP al servidor web interno en la dirección IPv4 192.168.1.254, con el número de puerto predeterminado 80.

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 (Puerto externo) en la ventana Single Port Forwarding (Reenvío de puerto único).

El enfoque adoptado para configurar el reenvío de puertos depende de la marca y el modelo del router de banda ancha en la red. No obstante, hay algunos pasos genéricos que se deben seguir. Si las instrucciones que suministra el ISP o las que vienen con el router no proporcionan una orientación adecuada, en el sitio web[http://www.portforward.com](http://www.portforward.com/) se ofrecen guías para varios routers de banda ancha. Puede seguir las instrucciones para agregar o eliminar puertos según sea necesario para satisfacer las necesidades de todas las aplicaciones que desee permitir o denegar.



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.

En la figura 1, se muestra el comando de NAT estática que se usa para configurar el reenvío de puertos con IOS.

En la figura 2, se muestra un ejemplo de configuración del reenvío de puertos con comandos de IOS en el router R2. La dirección 192.168.10.254 es la dirección IPv4 local interna del servidor web que escucha en el puerto 80. Los usuarios acceden a este servidor web interno con la dirección IP global 209.165.200.225, una dirección IPv4 pública globalmente única. En este caso, es la dirección de la interfaz Serial 0/1/0 del R2. El puerto global se configura como 8080. Este es el puerto de destino que se utiliza junto con la dirección IPv4 global 209.165.200.225 para acceder al servidor web interno. Observe los siguientes parámetros de comando dentro de la configuración NAT:

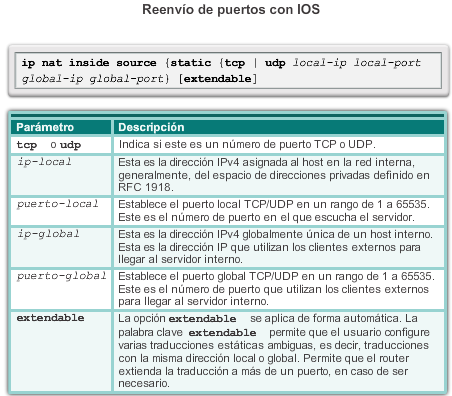
* *ip-local* = 192.168.10.254
* *puerto-local* = 80
* *ip-global* = 209.165.200.225
* *puerto-global* = 8080

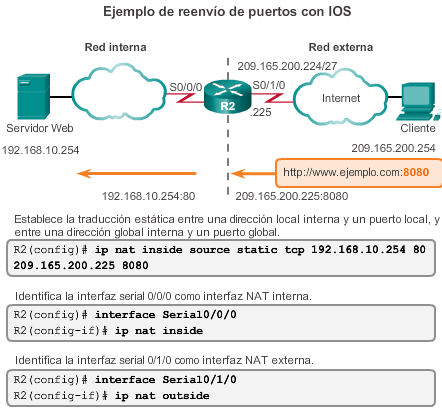
Cuando no se utiliza un número de puerto bien conocido, el cliente debe especificar el número de puerto de la aplicación.

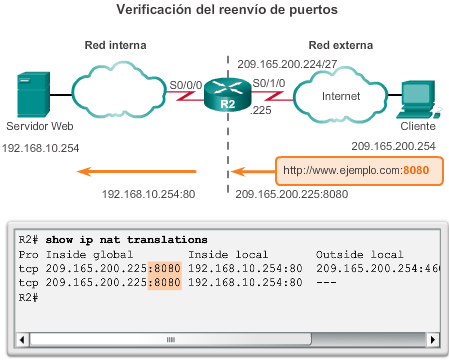
Al igual que otros tipos de NAT, el reenvío de puertos requiere que se configuren las interfaces NAT interna y externa.

Como en el caso de la NAT estática, se puede utilizar el comando **show ip nat translations** para verificar el reenvío de puertos, como se muestra en la figura 3.

En el ejemplo, cuando el router recibe el paquete con la dirección IPv4 global interna 209.165.200.225 y un puerto TCP de destino 8080, el router realiza una búsqueda en la tabla de NAT con la dirección IPv4 de destino y el puerto de destino como claves. A continuación, el router traduce la dirección a la dirección local interna del host 192.168.10.254 y el puerto de destino 80. Luego, el R2 reenvía el paquete al servidor web. En el caso de los paquetes de retorno del servidor web al cliente, este proceso se invierte.







### Configuración de NAT e IPv6

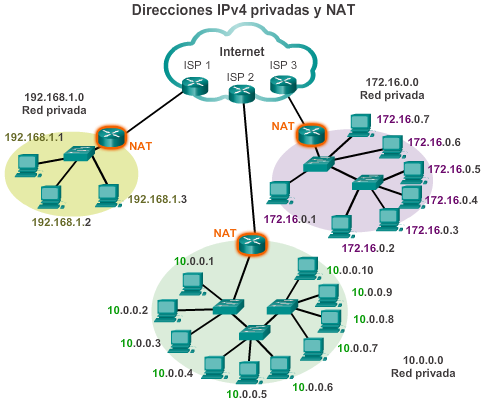
La cuestión del agotamiento del espacio de direcciones IPv4 es una prioridad para el IETF desde principios de la década de los noventa. La combinación de las direcciones IPv4 privadas definidas en RFC 1918 y de NAT cumple un papel decisivo para retrasar este agotamiento. NAT presenta desventajas considerables, y en enero de 2011, la IANA asignó sus últimas direcciones IPv4 a los RIR.

Uno de los beneficios de NAT para IPv4 que no fueron intencionales es que oculta la red privada de Internet pública. NAT tiene la ventaja de que ofrece un nivel de seguridad considerable al denegar el acceso de las computadoras que se encuentran en Internet pública a los hosts internos. Sin embargo, no debe considerarse como un sustituto de la seguridad de red adecuada, como la que proporciona un firewall.

En RFC 5902, el Consejo de Arquitectura de Internet (IAB) incluyó la siguiente cita sobre la traducción de direcciones de red IPv6:

“En general, se cree que una caja NAT proporciona un nivel de protección porque los hosts externos no pueden iniciar directamente una comunicación con los hosts detrás de una NAT. No obstante, no se deben confundir las cajas NAT con los firewalls. Como se analizó en [RFC4864], sección 2.2, el acto de traducción en sí mismo no proporciona seguridad. La función de filtrado con estado puede proporcionar el mismo nivel de protección sin requerir una función de traducción”.

Con una dirección de 128 bits, IPv6 proporciona 340 sextillones de direcciones. Por lo tanto, el espacio de direcciones no es un problema. IPv6 se desarrolló con la intención de que la NAT para IPv4 con su traducción entre direcciones IPv4 públicas y privadas resulte innecesaria. Sin embargo, IPv6 implementa una forma de NAT. IPv6 incluye su propio espacio de direcciones IPv6 privadas y NAT, que se implementan de manera distinta de como se hace para IPv4.



Las direcciones IPv6 locales únicas (ULA) se asemejan a las direcciones privadas en IPv4 definidas en RFC 1918, pero también existen diferencias considerables. El objetivo de las ULA es proporcionar espacio de direcciones IPv6 para las comunicaciones dentro de un sitio local, no tienen el propósito de proporcionar espacio adicional de direcciones IPv6 ni un nivel de seguridad.

Como se muestra en la ilustración, las ULA tienen el prefijo FC00::/7, lo que produce un rango de primer hexteto que va desde FC00 hasta FDFF. El bit siguiente se establece en 1 si el prefijo se asigna localmente. Es posible que en el futuro se pueda establecer en 0. Los 40 bits siguientes corresponden a una ID global seguida de una ID de subred de 16 bits. Estos primeros 64 bits se combinan para crear el prefijo de la ULA. Esto permite que los 64 bits restantes se utilicen para la ID de interfaz o, en términos de IPv4, la porción de host de la dirección.

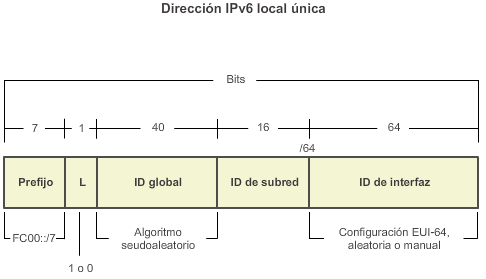
Las direcciones locales únicas se definen en RFC 4193. Las ULA también se conocen como “direcciones IPv6 locales” (no se deben confundir con las direcciones IPv6 link-local) y tienen varias características, incluidas las siguientes:

* Permiten que los sitios se combinen o se interconecten de manera privada, sin generar conflictos entre direcciones y sin necesidad de volver a numerar las interfaces que usan estos prefijos.
* Son independientes de cualquier ISP y se pueden usar para las comunicaciones dentro de un sitio sin tener conectividad a Internet.
* No se pueden enrutar a través de Internet; sin embargo, si se filtran por routing o DNS, no existe conflicto con otras direcciones.

Las ULA no son tan sencillas como las direcciones definidas en RFC 1918. A diferencia de las direcciones IPv4 privadas, el IETF no tenía la intención de utilizar una forma de NAT para traducir entre las direcciones locales únicas y las direcciones IPv6 de unidifusión global.

La comunidad de Internet continúa analizando la implementación y los posibles usos de las direcciones IPv6 locales únicas. Por ejemplo, el IETF considera permitir la opción de crear el prefijo de la ULA de forma local con FC00::/8, o de que lo asigne un tercero de forma automática y que empiece con FD00::/8.

**Nota:** la especificación original de IPv6 asignaba el espacio de direcciones para las direcciones locales de sitio, definidas en RFC 3513. El IETF dejó en desuso las direcciones locales de sitio en RFC 3879 porque el término “sitio” resultaba algo ambiguo. Las direcciones locales de sitio tenían el rango de prefijos FEC0::/10 y todavía pueden encontrarse en documentos antiguos de IPv6.

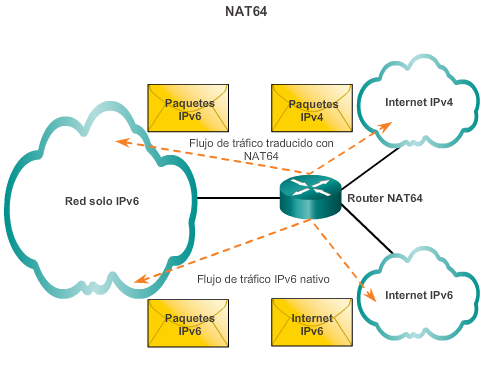


NAT para IPv6 se usa en un contexto muy distinto al de NAT para IPv4. Las variedades de NAT para IPv6 se usan para proporcionar acceso de manera transparente entre redes solo IPv6 y redes solo IPv4. No se utiliza como forma de traducción de IPv6 privada a IPv6 global.

Lo ideal es que IPv6 se ejecute de forma nativa siempre que sea posible. Es decir, en dispositivos IPv6 que se comunican entre sí a través de redes IPv6. No obstante, para colaborar en el cambio de IPv4 a IPv6, el IETF elaboró varias técnicas de transición que admiten una variedad de situaciones de IPv4 a IPv6, como dual-stack, tunneling y traducción.

Dual-stack es cuando los dispositivos ejecutan protocolos asociados a IPv4 y a IPv6. Tunneling para IPv6 es el proceso de encapsulación de un paquete IPv6 dentro de un paquete IPv4. Esto permite que el paquete IPv6 se transmita a través de una red solo IPv4.

La NAT para IPv6 no se debe usar como una estrategia a largo plazo, sino como un mecanismo temporal para contribuir a la migración de IPv4 a IPv6. Con el correr de los años, hubo varios tipos de NAT para IPv6, incluida la traducción de direcciones de red/traducción de protocolos (NAT-PT). El IETF dejó en desuso NAT-PT en favor de su reemplazo, NAT64. NAT64 excede el ámbito de este currículo.



## Resolución de problemas de NAT

En la figura 1, se muestra el R2 habilitado para PAT, que usa el rango de direcciones de 209.165.200.226 a 209.165.200.240.

Cuando hay problemas de conectividad IPv4 en un entorno NAT, suele ser difícil determinar la causa del problema. El primer paso para resolverlo es descartar que la causa sea NAT. Siga estos pasos para verificar que NAT funcione como se espera:

**Paso 1.** En función de la configuración, defina claramente lo que debe lograr la NAT. Esto puede revelar un problema con la configuración.

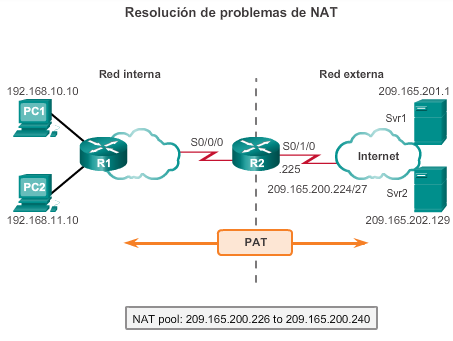
**Paso 2.** Verifique que las traducciones de la tabla sean correctas con el comando **show ip nat translations**.

**Paso 3.** Utilice los comandos **clear** y**debug** para verificar que NAT funcione como se espera. Verifique si se vuelven a crear las entradas dinámicas después de borrarlas.

**Paso 4.** Revise en detalle lo que sucede con el paquete y verifique que los routers tengan la información de routing correcta para trasladar el paquete.

En la figura 2, se muestra el resultado de los comandos **show ip nat statistics** y **show ip nat translations**. Antes de utilizar los comandos **show**, se eliminan las estadísticas y entradas de NAT de la tabla de NAT con los comandos **clear ip nat statistics** y **clear ip nat translation \***. Una vez que el host en 192.168.10.10 accede mediante Telnet al servidor en 209.165.201.1, se muestran las estadísticas de NAT y la tabla de NAT para verificar que NAT funcione como se espera.

En un entorno de red simple, es útil controlar las estadísticas de NAT con el comando **show ip nat statistics**. El comando **show ip nat statistics** muestra información sobre la cantidad total de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad que se asignó. Sin embargo, en un entorno NAT más complejo, con varias traducciones en curso, es posible que este comando no identifique el problema de forma clara. Es posible que se deban ejecutar los comandos **debug** en el router.



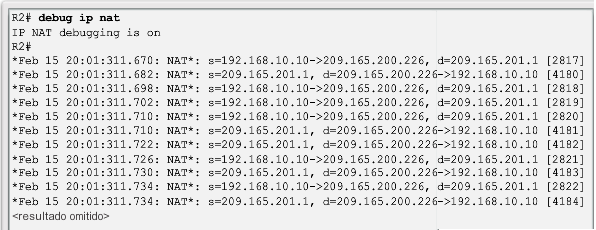
Para verificar el funcionamiento de la característica de NAT, utilice el comando**debug ip nat**, que muestra información sobre cada paquete que traduce el router. El comando **debug ip nat detailed**genera una descripción de cada paquete que se tiene en cuenta para traducir. Este comando también proporciona información sobre determinados errores o condiciones de excepción, como la falla para asignar una dirección global. El comando **debug ip nat detailed** genera más sobrecarga que el comando **debug ip nat**, pero puede proporcionar el detalle necesario para resolver el problema de NAT. Desactive siempre la depuración al finalizar.

En la figura 1, se muestra un resultado de ejemplo de **debug ip nat**. Este resultado muestra que el host interno (192.168.10.10) inició el tráfico hacia el host externo (209.165.201.1) y que la dirección de origen se tradujo a la dirección 209.165.200.226.

Cuando decodifique el resultado de este comando, observe los significados de los siguientes símbolos y valores:

* **\* (asterisco):** el asterisco junto a NAT indica que la traducción se realiza en la ruta de switching rápido. Al primer paquete en una conversación siempre se aplica el switching de procesos, que es más lento. Si existe una entrada de caché, el resto de los paquetes atraviesan la ruta de switching rápido.
* **s=:** este símbolo se refiere a la dirección IP de origen.
* **a.b.c.d**--->**w.x.y.z:** este valor indica que la dirección de origen a.b.c.d se traduce a w.x.y.z.
* **d=:** este símbolo se refiere a la dirección IP de destino.
* **[xxxx]:** el valor entre corchetes es el número de identificación IP. Esta información puede ser útil para la depuración, ya que habilita la correlación con otros seguimientos de paquetes realizados por los analizadores de protocolos.

**Nota:** verifique que la ACL mencionada en la referencia de comandos de NAT permita todas las redes necesarias. En la figura 2, solo las direcciones 192.168.0.0/16 se pueden traducir. El R2 no traduce los paquetes de la red interna destinados a Internet con direcciones de origen que la ACL 1 no permita de forma explícita.



**Caso práctico 1**

En la figura 1, se muestra que los hosts de las LAN 192.168.0.0/16, la PC1 y la PC2, no pueden hacer ping a los servidores en la red externa, el Svr1 y el Svr2.

Para iniciar la resolución de problemas, utilice el comando **show ip nat translations** a fin de verificar si actualmente hay alguna traducción en la tabla de NAT. El resultado de la figura 1 muestra que no hay traducciones en la tabla.

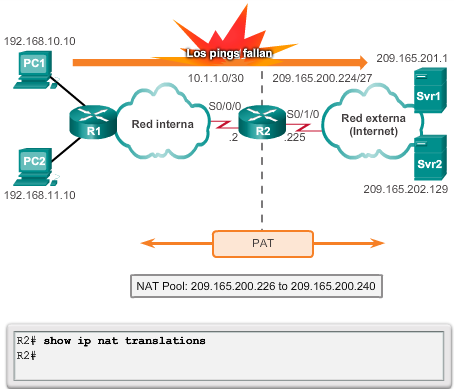
El comando **show ip nat statistics**se utiliza para determinar si se realizaron traducciones. También identifica las interfaces entre las que debe ocurrir la traducción. Como se muestra en el resultado de la figura 2, los contadores de NAT están en 0, lo que verifica que no se realizó ninguna traducción. Al comparar el resultado con la topología de la figura 1, observe que las interfaces del router están definidas de forma incorrecta como NAT interna o NAT externa. También es posible verificar una configuración incorrecta con el comando **show running-config**.

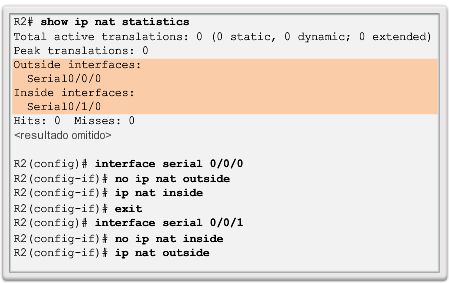
Se debe eliminar la configuración NAT actual de las interfaces antes de aplicar la configuración correcta.

Luego de definir correctamente las interfaces NAT interna y externa, otro ping de la PC1 al Svr1 falla. El uso de los comandos **show ip nat translations** y **show ip nat statistics** nuevamente verifica que no hay traducciones en curso.

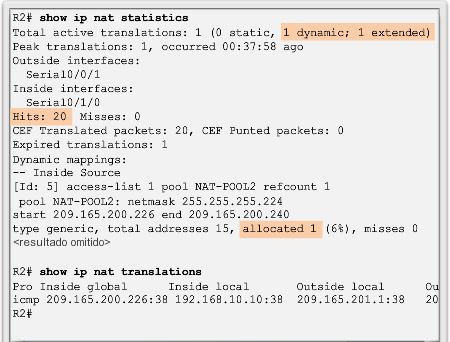
Como se muestra en la figura 3, el comando **show access-lists** se utiliza para determinar si la ACL a la que hace referencia el comando NAT permite todas las redes necesarias. Al examinar el resultado, se comprueba que se utilizó una máscara de bits wildcard incorrecta en la ACL que define las direcciones que se deben traducir. La máscara wildcard solo permite la subred 192.168.0.0/24. Primero se elimina la lista de acceso y después se reconfigura con la máscara wildcard correcta.

Una vez corregidas las configuraciones, se genera otro ping de la PC1 al Svr1, y esta vez el ping es correcto. Como se muestra en la figura 4, los comandos **show ip nat translations** y **show ip nat statistics** se utilizan para verificar que se produzca la traducción NAT.









## Resumen

En este capítulo, se explicó cómo se utiliza NAT para contribuir a mitigar el agotamiento del espacio de direcciones IPv4. La NAT para IPv4 permite que los administradores de red utilicen el espacio de direcciones privadas definido en RFC 1918, a la vez que proporciona conectividad a Internet, mediante una única dirección pública o una cantidad limitada de estas.

NAT conserva el espacio de direcciones públicas y reduce la sobrecarga administrativa de forma considerable al administrar las adiciones, los movimientos y las modificaciones. NAT y PAT se pueden implementar para ahorrar espacio de direcciones públicas y armar intranets privadas seguras sin afectar la conexión al ISP. Sin embargo, NAT presenta desventajas en términos de sus efectos negativos en el rendimiento de los dispositivos, la seguridad, la movilidad y la conectividad de extremo a extremo, y se debe considerar como una implementación a corto plazo para el agotamiento de direcciones, cuya solución a largo plazo es IPv6.

En este capítulo, se analizó la NAT para IPv4, incluido lo siguiente:

* Las características, la terminología y las operaciones generales de NAT
* Los diferentes tipos de NAT, incluidas la NAT estática, la NAT dinámica y PAT
* Las ventajas y las desventajas de NAT
* La configuración, la verificación y el análisis de la NAT estática, la NAT dinámica y PAT
* La forma en que se puede usar el reenvío de puertos para acceder a los dispositivos internos desde Internet
* La resolución de problemas de NAT mediante los comandos **show** y**debug**



