

Configuración de Network Address Translation: Getting Started

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Pasos de Inicio Rápido para Configurar e Implementar NAT](#)

[Definición de Interfaces NAT Interiores y Exteriores](#)

[Ejemplo: Permiso para que los Usuarios Internos Accedan a Internet](#)

[Configuración de NAT para Permitir que los Usuarios Internos Accedan a Internet](#)

[Configuración de NAT para Permitir que los Usuarios Internos Accedan a Internet Usando Sobrecarga](#)

[Ejemplo: Permiso para el Acceso a Dispositivos Interiores desde Internet](#)

[Configuración de NAT para Permitir el Acceso a Dispositivos Internos desde Internet](#)

[Ejemplo: Redirección del Tráfico de TCP a Otro Puerto o Dirección TCP](#)

[Configuración de NAT para Redireccionar el Tráfico TCP a otro Puerto o Dirección TCP](#)

[Ejemplo: Uso de NAT Durante una Transición de Red](#)

[Configuración del Uso de NAT Durante una Transición de Red](#)

[Ejemplo: Utilización de NAT en Redes Superpuestas](#)

[Diferencia entre Mapping Uno a Uno y Múltiple](#)

[Verificación de Funcionamiento de NAT](#)

[Conclusión](#)

[Información Relacionada](#)

[Introducción](#)

En este documento se explica cómo configurar el proceso Network Address Translation (NAT) en un router Cisco para su uso en escenarios de redes frecuentes. Este documento está dirigido a quienes utilizan NAT por primera vez.

Note: En este documento, cuando se hace referencia a Internet o a un dispositivo de Internet, se está haciendo referencia a un dispositivo de cualquier red externa.

[prerrequisitos](#)

[Requisitos](#)

Para entender este documento, hay que tener un conocimiento básico de los términos que se utilizan en relación con NAT. Algunas de las definiciones se pueden encontrar en [NAT: Definiciones Locales y Globales](#).

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Cisco 2500 Series Routers

Versión 12.2(10b) del software del IOS® de Cisco

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

[Pasos de Inicio Rápido para Configurar e Implementar NAT](#)

En ocasiones, cuando se configura el proceso NAT, resulta difícil saber por dónde empezar, especialmente si no se tienen conocimientos al respecto. Los pasos incluidos a continuación lo guiarán para definir qué quiere que realice NAT y cómo configurar este proceso:

[Defina las interfaces NAT interiores y exteriores.](#)

¿Existen usuarios fuera de las interfaces múltiples?

¿Hay varias interfaces que van a Internet?

Defina qué está tratando de lograr con NAT.

¿Está intentando [permitir que los usuarios internos accedan a Internet](#)?

¿Está intentando [permitir que Internet acceda a los dispositivos internos](#) (como el servidor de correo o el servidor Web)?

¿Está intentando [redireccionar el tráfico TCP a otro puerto o a otra dirección TCP](#)?

¿Está utilizando [durante una transición en la red](#) (por ejemplo, usted cambió la dirección IP de un servidor y quiere que los clientes no actualizados puedan acceder al servidor con la dirección IP original hasta actualizar a todos los clientes y que los clientes actualizados puedan acceder al servidor con la nueva dirección)?

¿Está utilizando NAT para [permitir que las redes superpuestas se comuniquen](#)?

Configure NAT para poder lograr lo que definió arriba. De acuerdo con lo que definió en el paso 2, debe determinar cuál de las siguientes funciones utilizará:

NAT estática

NAT dinámica

Sobrecarga

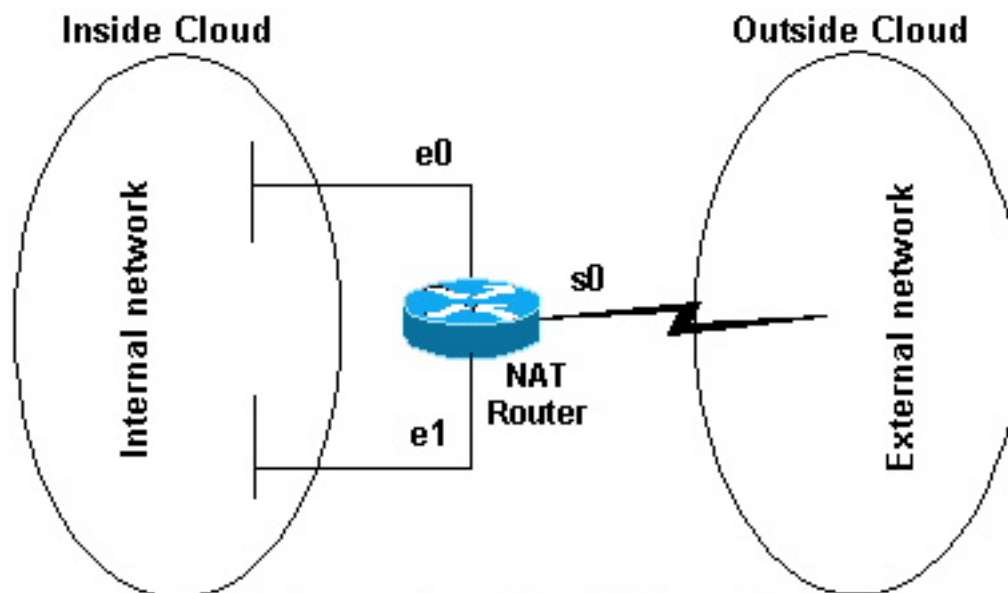
Cualquier combinación de las opciones anteriores

Verifique el funcionamiento de NAT.

Cada uno de estos ejemplos de NAT lo guían en los pasos 1 a 3 de los Pasos de Inicio Rápido presentados arriba. Estos ejemplos describen algunos escenarios frecuentes en los cuales Cisco recomienda la implementación de NAT.

Definición de Interfaces NAT Interiores y Exteriores

El primer paso de la implementación de NAT consiste en definir las interfaces NAT interiores y exteriores. Puede ser que le resulte más fácil definir su red interna como interior y la red externa como exterior. Sin embargo, los términos interno y externo también están sujetos a decisión. Esta figura muestra un ejemplo de esto.



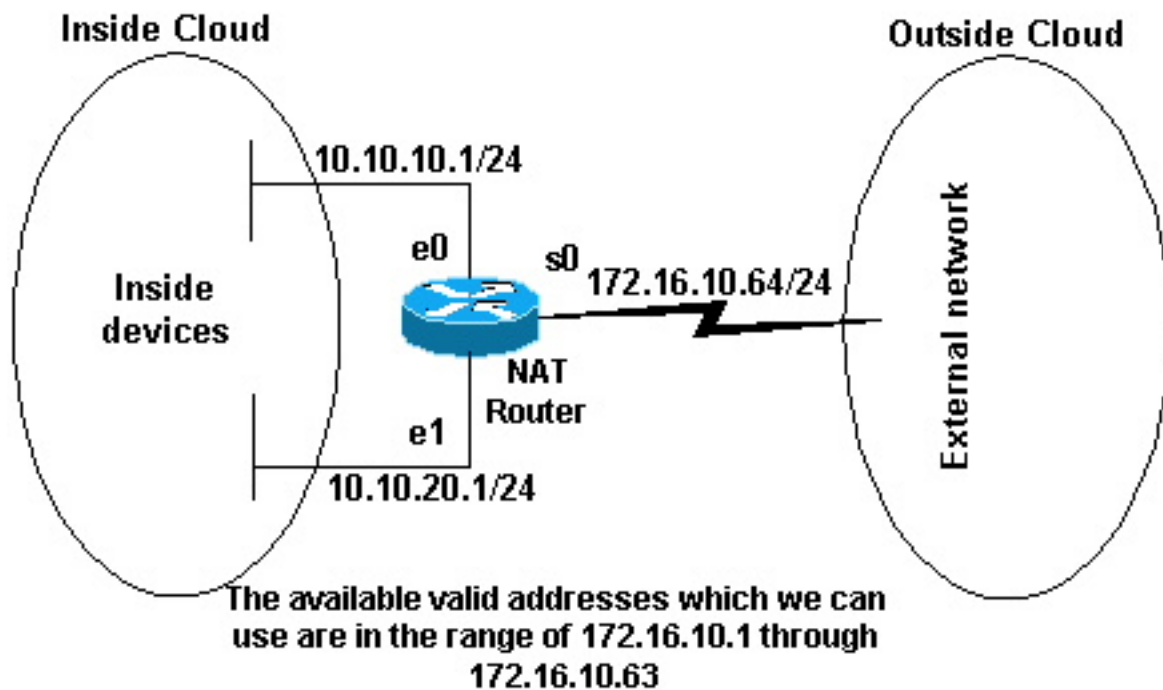
In this figure, ethernet 0 and ethernet 1 will be defined as NAT inside interfaces and serial 0 will be defined as a NAT outside interface.

Ejemplo: Permiso para que los Usuarios Internos Accedan a

Internet

Es posible que quiera permitirles a los usuarios internos acceder a Internet, pero quizá no tenga direcciones válidas suficientes para admitir a todos ellos. Si toda la comunicación con los dispositivos en Internet es iniciada por los dispositivos internos, usted necesita una sola dirección válida o un conjunto de direcciones válidas.

Este es un diagrama de red simple con las interfaces del router definidas como interiores y exteriores:



En este ejemplo, usted quiere que NAT les permita a ciertos dispositivos (los primeros 31 de cada subred) del interior iniciar comunicación con los dispositivos del exterior mediante la traducción de su dirección no válida a una dirección válida o a un conjunto de direcciones. El conjunto se ha definido como el rango de las direcciones de 172.16.10.1 a 172.16.10.63.

Ahora está listo para configurar NAT. Para lograr lo definido arriba, utilice NAT dinámica. Con NAT dinámica, la tabla de traducción en el router está inicialmente vacía y se completa una vez que el tráfico que necesita ser traducido pasa por el router. Esto se opone a la NAT estática, en la que una traducción se configura estáticamente y se coloca en la tabla de traducción sin la necesidad de ningún tráfico.

En este ejemplo, puede configurar NAT para traducir cada uno de los dispositivos interiores a una sola dirección válida o para traducir cada uno de los dispositivos interiores a la misma dirección válida. Este segundo método se conoce como sobrecarga. Aquí se incluye un ejemplo de cómo configurar cada método.

Configuración de NAT para Permitir que los Usuarios Internos Accedan a Internet

Router NAT

```
interface ethernet 0
 ip address 10.10.10.1 255.255.255.0
```

```

ip nat inside
!--- Defines Ethernet 0 with an IP address and as a NAT
inside interface. interface ethernet 1 ip address
10.10.20.1 255.255.255.0 ip nat inside !--- Defines
Ethernet 1 with an IP address and as a NAT inside
interface. interface serial 0 ip address 172.16.10.64
255.255.255.0 ip nat outside !--- Defines serial 0 with
an IP address and as a NAT outside interface. ip nat
pool no-overload 172.16.10.1 172.16.10.63 prefix 24 ! !-
-- Defines a NAT pool named no-overload with a range of
addresses !--- 172.16.10.1 - 172.16.10.63. ip nat inside
source list 7 pool no-overload ! ! !--- Indicates that
any packets received on the inside interface that !---
are permitted by access-list 7 has !--- the source
address translated to an address out of the !--- NAT
pool "no-overload". access-list 7 permit 10.10.10.0
0.0.0.31 access-list 7 permit 10.10.20.0 0.0.0.31 !---
Access-list 7 permits packets with source addresses
ranging from !--- 10.10.10.0 through 10.10.10.31 and
10.10.20.0 through 10.10.20.31.

```

Note: Cisco recomienda encarecidamente que no configure listas de acceso a las que hagan referencia los comandos NAT con la opción **permit any**. El uso de **permit any** puede hacer que NAT consuma demasiados recursos del router, lo que puede ocasionar problemas en la red.

Observe que en la configuración anterior solamente las primeras 32 direcciones de la subred 10.10.10.0 y las primeras 32 direcciones de la subred 10.10.20.0 son permitidas por **access-list 7**. Por lo tanto, solo se traducen estas direcciones de origen. Puede haber otros dispositivos con otras direcciones en la red interior, pero estas no se traducen.

El último paso es verificar que [NAT esté funcionando correctamente](#).

[Configuración de NAT para Permitir que los Usuarios Internos Accedan a Internet Usando Sobrecarga](#)

```

Router NAT

interface ethernet 0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!--- Defines Ethernet 0 with an IP address and as a NAT
inside interface. interface ethernet 1 ip address
10.10.20.1 255.255.255.0 ip nat inside !--- Defines
Ethernet 1 with an IP address and as a NAT inside
interface. interface serial 0 ip address 172.16.10.64
255.255.255.0 ip nat outside !--- Defines serial 0 with
an IP address and as a NAT outside interface. ip nat
pool ovrlld 172.16.10.1 172.16.10.1 prefix 24 ! !---
Defines a NAT pool named ovrlld with a range of a single
IP !--- address, 172.16.10.1. ip nat inside source list
7 pool ovrlld overload ! ! ! ! !--- Indicates that any
packets received on the inside interface that !--- are
permitted by access-list 7 has the source address !---
translated to an address out of the NAT pool named
ovrlld. !--- Translations are overloaded, which allows
multiple inside !--- devices to be translated to the
same valid IP address. access-list 7 permit 10.10.10.0
0.0.0.31 access-list 7 permit 10.10.20.0 0.0.0.31 !---
Access-list 7 permits packets with source addresses
ranging from !--- 10.10.10.0 through 10.10.10.31 and

```

10.10.20.0 through 10.10.20.31.

Observe que, en la segunda configuración de arriba, el conjunto NAT "ovrld" solamente tiene un rango de una dirección. La palabra clave sobrecarga usada en el comando `ip nat inside source list 7 pool ovrld overload` permite que NAT traduzca múltiples dispositivos interiores a la única dirección en el conjunto.

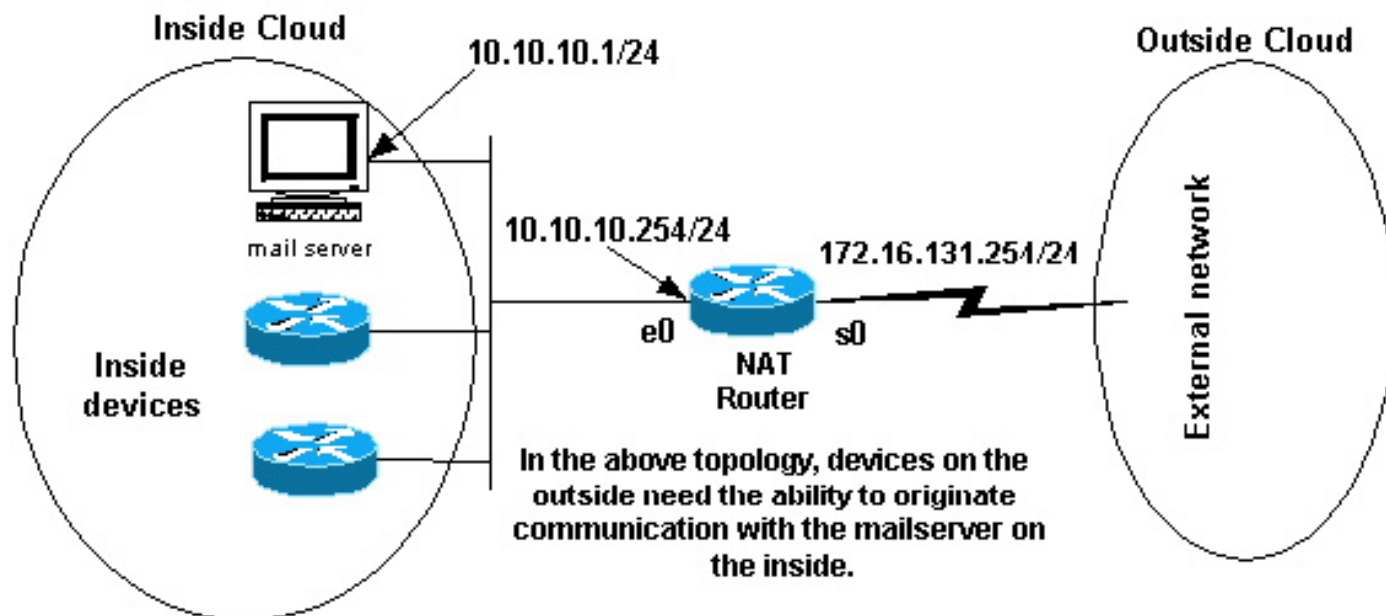
Otra variación de este comando es `ip nat inside source list 7 interface serial 0 overload`, que configura NAT para sobrecarga en la dirección que está asignada a la interfaz 0 serial.

Cuando se configura la función de sobrecarga, el router mantiene información suficiente de protocolos de mayor nivel (por ejemplo, los números del puerto TCP o UDP) a fin de traducir la dirección global para que vuelva a ser la dirección local correcta. Para obtener las definiciones de dirección global y de dirección local, consulte [NAT: Definiciones de Direcciones Globales y Locales](#).

El último paso es verificar que [NAT esté funcionando correctamente](#).

Ejemplo: Permiso para el Acceso a Dispositivos Interiores desde Internet

Puede necesitar dispositivos internos para intercambiar información con los dispositivos en Internet, donde se inicia la comunicación desde los dispositivos de Internet, por ejemplo, el correo electrónico. Es típica para los dispositivos en Internet enviar el correo electrónico a un mail server que resida en la red interna.



Configuración de NAT para Permitir el Acceso a Dispositivos Internos desde Internet

En este ejemplo, primero define las interfaces NAT interiores y exteriores, tal como se muestra en el diagrama de red anterior.

En segundo lugar, define que quiere que los usuarios en el interior puedan iniciar comunicación con el exterior. Los dispositivos en el exterior deben poder iniciar comunicación con únicamente el

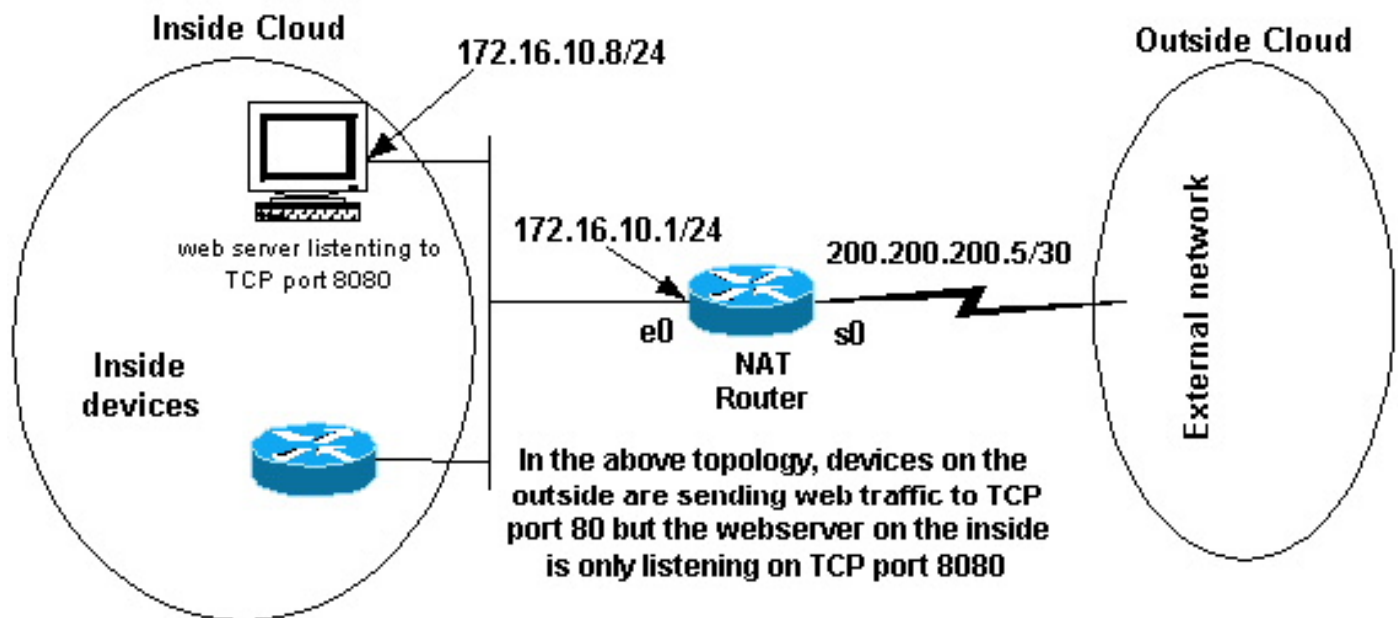
servidor de correo en el interior.

El tercer paso es configurar NAT. Para lograr lo que ha definido, puede configurar NAT estática y NAT dinámica simultáneamente. Para obtener más información sobre cómo configurar este ejemplo, consulte [Configuración Simultánea de NAT Estática y de NAT Dinámica](#).

El último paso es verificar que [NAT esté funcionando correctamente](#).

Ejemplo: Redirección del Tráfico de TCP a Otro Puerto o Dirección TCP

Tener un servidor web en una red interna es otro ejemplo de cuándo podría ser necesario que los dispositivos en Internet inicien comunicación con los dispositivos internos. El servidor web interno se puede configurar en algunos casos para escuchar el tráfico web en un puerto TCP diferente al puerto 80. Por ejemplo, el servidor web interno se puede configurar para escuchar el puerto TCP 8080. En este caso, puede usar NAT para redirigir el tráfico destinado al puerto TCP 80 al puerto TCP 8080.



Después de definir las interfaces tal como se muestra en el diagrama de red anterior, puede decidir que quiere que NAT redireccione los paquetes del exterior destinados a 172.16.10.8:80 a 172.16.10.8:8080. Puede utilizar un **comando static nat** para traducir el número del puerto TCP a fin de lograr lo que desea. Un configuración se muestra aquí a modo de ejemplo.

Configuración de NAT para Redireccionar el Tráfico TCP a otro Puerto o Dirección TCP

```
Router NAT

interface ethernet 0
 ip address 172.16.10.1 255.255.255.0
 ip nat inside
 !--- Defines Ethernet 0 with an IP address and as a NAT
 inside interface. interface serial 0 ip address
 200.200.200.5 255.255.255.252 ip nat outside !---
 Defines serial 0 with an IP address and as a NAT outside
```

```
interface. ip nat inside source static tcp 172.16.10.8
8080 172.16.10.8 80 !--- Static NAT command that states
any packet received in the inside !--- interface with a
source IP address of 172.16.10.8:8080 is !--- translated
to 172.16.10.8:80.
```

Observe que la descripción de la configuración para el comando static NAT indica que cualquier paquete recibido en la interfaz interior con una dirección de origen de 172.16.10.8:8080 es traducido a 172.16.10.8:80. Esto también implica que cualquier paquete recibido en la interfaz exterior con una dirección de destino de 172.16.10.8:80 tenga el destino traducido a 172.16.10.8:8080.

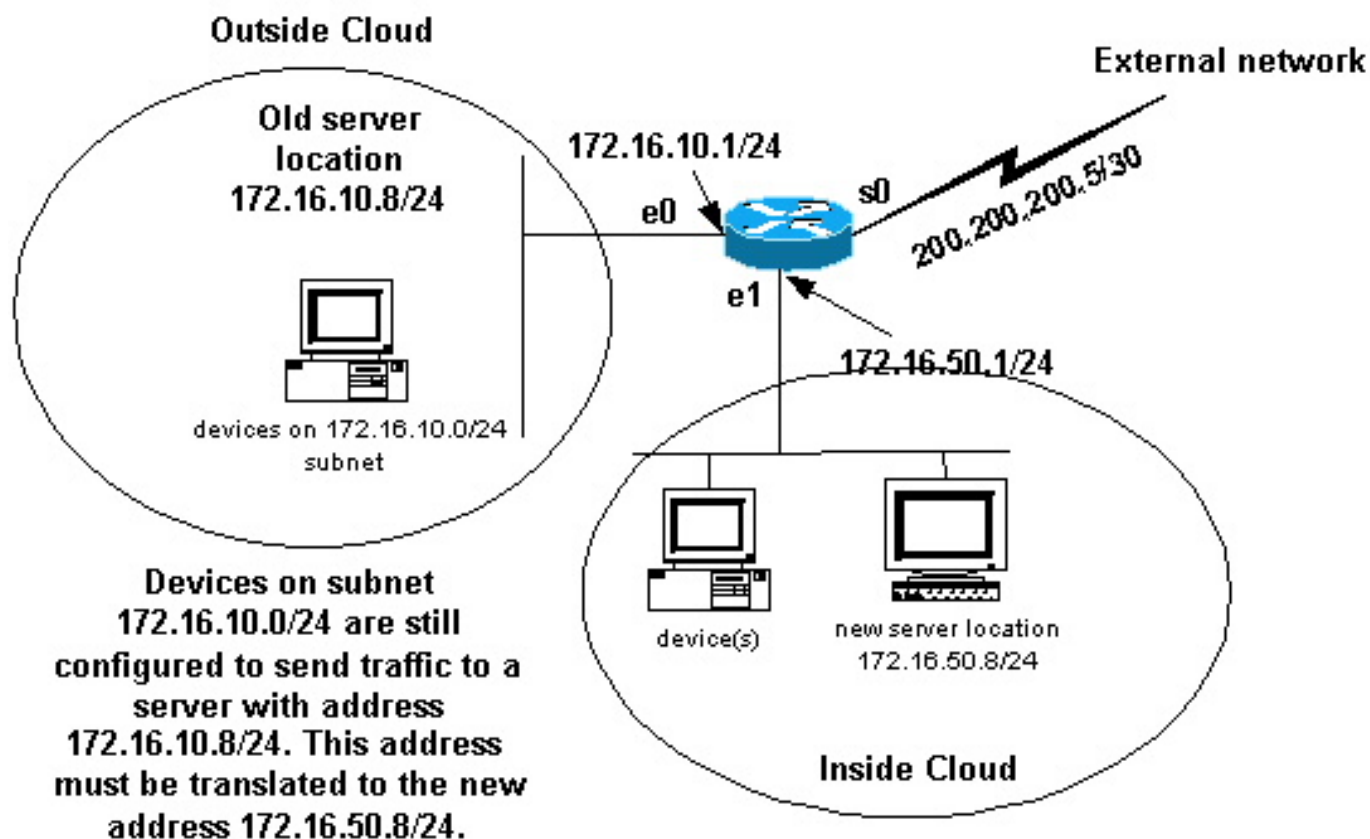
El último paso es verificar que [NAT esté funcionando correctamente](#).

```
show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
tcp	172.16.10.8:80	172.16.10.8:8080	---	---

Ejemplo: Uso de NAT Durante una Transición de Red

La implementación de NAT resulta útil cuando necesita redireccionar los dispositivos en la red o cuando sustituye un dispositivo por otro. Por ejemplo, si todos los dispositivos en la red utilizan un servidor determinado y este servidor debe ser sustituido por un nuevo con una nueva dirección IP, la reconfiguración de todos los dispositivos de red para que utilicen la nueva dirección del servidor lleva un tiempo. Mientras tanto, usted puede utilizar NAT para configurar los dispositivos con la dirección vieja a fin de traducir sus paquetes para que se comuniquen con el nuevo servidor.



Después de definir las interfaces NAT como se muestra arriba, puede decidir que quiere que NAT permita que los paquetes del exterior con destino a la vieja dirección del servidor (172.16.10.8) sean traducidos y enviados a la nueva dirección del servidor. Observe que el nuevo servidor está

en una LAN diferente y que los dispositivos en esta LAN o cualquier dispositivo alcanzable a través de esta LAN (dispositivos en la parte interior de la red) deberían ser configurados para utilizar la dirección IP del nuevo servidor, de ser posible.

Puede utilizar NAT estática para lograr lo que desea. Este es un ejemplo de configuración.

Configuración del Uso de NAT Durante una Transición de Red

```
Router NAT

interface ethernet 0
 ip address 172.16.10.1 255.255.255.0
 ip nat outside
 !--- Defines Ethernet 0 with an IP address and as a NAT
 outside interface. interface ethernet 1 ip address
 172.16.50.1 255.255.255.0 ip nat inside !--- Defines
 Ethernet 1 with an IP address and as a NAT inside
 interface. interface serial 0 ip address 200.200.200.5
 255.255.255.252 !--- Defines serial 0 with an IP
 address. This interface is not !--- participating in
 NAT. ip nat inside source static 172.16.50.8 172.16.10.8
 !--- States that any packet received on the inside
 interface with a !--- source IP address of 172.16.50.8
 is translated to 172.16.10.8.
```

Observe que el comando inside source NAT en este ejemplo también implica que los paquetes recibidos en la interfaz exterior con una dirección de destino de 172.16.10.8 tengan la dirección de destino traducida a 172.16.50.8.

El último paso es verificar que [NAT esté funcionando correctamente](#).

Ejemplo: Utilización de NAT en Redes Superpuestas

Cuando asigna direcciones IP a los dispositivos internos que ya están siendo utilizados por otros dispositivos en Internet, se produce una superposición de redes. También se superponen redes cuando dos compañías, que utilizan direcciones IP [RFC 1918](#) en sus redes, se fusionan. [Estas dos redes necesitan comunicarse, preferentemente sin tener que redirigir todos los dispositivos](#). Consulte [Uso de NAT en Redes Superpuestas](#) para obtener más información sobre la configuración de NAT con esta finalidad.

Diferencia entre Mapping Uno a Uno y Múltiple

Una configuración NAT estática crea un mapping uno a uno y traduce a una dirección específica a otra dirección. Este tipo de configuración crea una entrada permanente en la tabla NAT siempre que la configuración esté presente y habilita los hosts internos y externos para iniciar la conexión. Esta configuración es particularmente útil para los hosts que brindan servicios de aplicación, como correo, web y FTP, entre otros. Por ejemplo:

```
Router(config)#ip nat inside source static 10.3.2.11 10.41.10.12
Router(config)#ip nat inside source static 10.3.2.12 10.41.10.13
```

NAT dinámica es útil cuando la cantidad de direcciones disponibles es inferior al número real de hosts por traducir. Crea una entrada en la tabla de NAT cuando el host inicia una conexión y establece un mapping uno a uno entre las direcciones. No obstante, el mapping puede variar y

depende de la dirección registrada disponible en el conjunto en el momento de la comunicación. NAT dinámica permite que las sesiones sean iniciadas solamente desde redes interiores o exteriores para las cuales se configura. Las entradas de NAT dinámica se quitan de la tabla de traducción si el host no se comunica durante un período específico que es configurable. Luego la dirección vuelve al conjunto para que la use otro host.

Por ejemplo, complete estos pasos de la configuración detallada:

Cree un conjunto de direcciones.

```
Router(config)#ip nat pool MYPOOLEXAMPLE
10.41.10.1 10.41.10.41 netmask 255.255.255.0
```

Cree una lista de acceso para las redes interiores a las que deba aplicarse mapping.

```
Router(config)#access-list 100 permit ip
10.3.2.0 0.0.0.255 any
```

Asocie la lista de acceso 100 que está seleccionando la red interna 10.3.2.0 0.0.0.255 a la que se debe aplicar NAT con el conjunto MYPOOLEXAMPLE y luego sobrecargue las direcciones.

```
Router(config)#ip nat inside source list 100 pool
MYPOOLEXAMPLE overload
```

[Verificación de Funcionamiento de NAT](#)

Después de configurar el proceso NAT, verifique que funcione correctamente. Puede hacer esto de diversas maneras: usando un analizador de red, los **comandos show** o los **comandos debug**. Para obtener un ejemplo detallado de la verificación de NAT, consulte [Verificación del Funcionamiento de NAT y Troubleshooting de NAT básica](#).

[Conclusión](#)

Los ejemplos incluidos en este documento demuestran pasos de inicio rápido que pueden ayudarlo a configurar y a implementar el proceso NAT. Estos pasos de inicio rápido incluyen:

Definición de interfaces NAT interiores y exteriores.

Definición de lo que intenta lograr con NAT.

Configuración de NAT para lograr lo que definió en el Paso 2.

Verificación del funcionamiento de NAT.

En cada uno de los ejemplos anteriores, se utilizaron diversas formas del **comando ip nat inside** . También puede utilizar el **comando ip nat outside** para lograr los mismos objetivos, pero tenga presente el orden de funcionamiento de NAT. Para los ejemplos de configuración que utilizan los **comandos ip nat outside**, consulte [Ejemplo de Configuración con el Comando ip nat outside source list](#) y [Ejemplo de Configuración con el Comando ip nat outside source static](#).

Los ejemplos anteriores también demostraron estas acciones:

Comando	Acción
fuelle interior nacional del IP	<ul style="list-style-type: none">• Traduce el origen de los paquetes IP que viajan desde adentro hacia afuera.• Traduce el destino de los paquetes IP que viajan desde afuera hacia adentro.
fuelle externa nacional del IP	<ul style="list-style-type: none">• Traduce el origen de los paquetes IP que viajan desde afuera hacia adentro.• Traslada el destino de los paquetes IP que están viajando del interior al exterior.

[Información Relacionada](#)

- [Página de Soporte de NAT](#)
- [Página de Soporte de IP Routed Protocols](#)
- [Página de Soporte de IP Routing](#)
- [Cómo Funciona NAT](#)
- [Orden de Funcionamiento de NAT](#)
- [Preguntas Frecuentes sobre la NAT del IOS de Cisco](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)