

# Revisión sobre las preguntas frecuentes sobre la Traducción de direcciones de red (NAT)

## Contenido

---

### [Introducción](#)

### [NAT genérica](#)

[P. ¿Qué significa "NAT"?](#)

[P. ¿Cómo funciona la NAT?](#)

[P. ¿Cómo se configura la NAT?](#)

[P. ¿Cuáles son las diferencias principales entre las implementaciones de NAT del Cisco IOS Software y Cisco PIX Security Appliance?](#)

[P. ¿Con qué hardware de routing Cisco se ofrece la NAT en Cisco IOS? ¿Cómo se puede comprar el hardware?](#)

[P. ¿La NAT ocurre antes o después del ruteo?](#)

[P. ¿Se puede implementar la NAT en un entorno de LAN inalámbrica pública?](#)

[P. ¿La NAT hace equilibrio de carga del protocolo TCP para servidores en la red interna?](#)

[P. ¿Puedo limitar la cantidad de NAT?](#)

[P. ¿Cómo se aprende o propaga el routing en direcciones o subredes IP empleadas por la NAT?](#)

[P. ¿Cuántas sesiones NAT concurrentes admite Cisco IOS NAT?](#)

[P. ¿Qué tipo de rendimiento de routing puede esperarse al usar la NAT de Cisco IOS?](#)

[P. ¿La NAT de Cisco IOS puede aplicarse en subinterfaces?](#)

[P. ¿La NAT de Cisco IOS puede usarse con el protocolo de router de reserva activa \(HSRP\) para ofrecer enlaces redundantes a un proveedor de servicios de Internet \(ISP\)?](#)

[P. ¿La NAT de Cisco IOS admite traducciones entrantes en una interfaz de retransmisión de tramas? ¿Es compatible con las traducciones de salida en el lado Ethernet?](#)

[P. ¿Un router con la NAT activada puede permitir que algunos usuarios empleen la NAT y otros usuarios de la misma interfaz Ethernet continúen usando sus propias direcciones IP?](#)

[P. Al configurar la PAT \(sobrecarga\), ¿cuál es la cantidad máxima de traducciones que pueden crearse por dirección IP global interna?](#)

[P. ¿Cómo funciona la PAT?](#)

[P. ¿Qué son los grupos de IP de la NAT?](#)

[P. ¿Cuál es el número máximo de agrupaciones IP de NAT configurables \(ip nat pool \)?](#)

[P. ¿Cuál es la ventaja de usar un mapa de rutas en lugar de una ACL en un grupo de NAT?](#)

[P. ¿Qué es la superposición de direcciones IP en el contexto de NAT?](#)

[P. ¿Qué son las NAT estáticas?](#)

[P. ¿Qué se entiende por el término sobrecarga de NAT? ¿Es PAT?](#)

[P. ¿Qué son las NAT dinámicas?](#)

[P. ¿Qué es ALG?](#)

[P. ¿Es posible crear una configuración con NAT estáticas y dinámicas?](#)

[P. Cuando un traceroute se realiza a través de un router NAT, ¿traceroute muestra la dirección NAT-Global o filtra la dirección NAT-Local?](#)

[P. ¿Cómo asigna puertos la PAT?](#)

[P. ¿Cuál es la diferencia entre la fragmentación de IP y la segmentación del protocolo TCP?](#)

[P. ¿La NAT admite la fragmentación de IP y la segmentación del protocolo TCP fuera de orden?](#)

[P. ¿Cómo se depuran la fragmentación de IP y la segmentación del protocolo TCP?](#)

[P. ¿Hay alguna MIB de NAT compatible?](#)

[P. ¿Qué es el tiempo de espera del protocolo TCP y cómo se relaciona con el temporizador del protocolo TCP de NAT?](#)

[P. ¿Puedo cambiar la cantidad de tiempo que tarda una traducción NAT a tiempo de espera de la tabla de traducción NAT?](#)

[P. ¿Cómo impido que el protocolo ligero de acceso a directorios \(LDAP\) adjunte bytes adicionales en cada paquete de respuesta del protocolo LDAP?](#)

[P. ¿Cuál es la ruta recomendada para la dirección IP global interna/local externa en la caja de NAT?](#)

[P. ¿La NAT de Cisco IOS soporta las ACL con una palabra clave de registro?](#)

## NAT de voz

[P. ¿La NAT admite Skinny Client Control Protocol \(SCCP\) v17 que viene con Cisco Unified Communications Manager \(CUCM\) V7?](#)

[P. ¿Qué versiones de carga de CUCM/SCCP/firmware admite la NAT?](#)

[P. ¿Qué es la mejora de asignación de puertos de la PAT de proveedores de servicios para los protocolos RTP y RTCP?](#)

[P. ¿Qué es el protocolo de inicio de sesión \(SIP\)? ¿Se puede usar la NAT con paquetes de protocolo SIP?](#)

[P. ¿Qué es la compatibilidad de NAT transversal en host con controladores de límites de sesión \(SBC\)?](#)

[P. ¿Cuántas llamadas de SIP, Skinny y H323 admiten la CPU y la memoria del router con la NAT?](#)

[P. ¿Un router NAT soporta la segmentación TCP de los paquetes Skinny y H323?](#)

[P. ¿Hay que prestar atención a algo al emplear una configuración de sobrecarga de NAT en una implementación de voz?](#)

[P. ¿Se conocen problemas causados por el empleo del comando clear ip nat trans \\* o clear ip nat trans forced en implementaciones de voz?](#)

[P. ¿La NAT admite la solución de coubicación de voz?](#)

[P. ¿La NVI admite el ALG de Skinny, H323 o el protocolo TCP SIP?](#)

## NAT con VRF/MPLS

[P. ¿Un router NAT soporta alguna vez NATting en el mismo espacio de dirección en un VRF al mismo tiempo que NATted en un espacio de dirección global? Actualmente, recibo esta advertencia: "% similar static entry \(10.1.1.1 -> 10.210.2.2\) already exists" cuando intento configurar esto:](#)

[P. ¿Las NAT antiguas admiten VRF-Lite \(NAT del VRF a otro VRF\)?](#)

## NAT NVI

[P. ¿Qué es NAT NVI?](#)

[P. ¿Se debe utilizar NAT NVI al realizar NAT entre una interfaz en global y una interfaz en un VRF?](#)

[P. ¿Se admite la segmentación del protocolo TCP para NAT-NVI?](#)

[P. ¿La NVI admite el ALG de Skinny, H323 o el protocolo TCP SIP?](#)

[P. ¿Se admite la segmentación del protocolo TCP con la SNAT?](#)

## SNAT

[P. ¿Qué es la NAT con estado \(SNAT\)?](#)

[P. ¿Se admite la segmentación del protocolo TCP con la SNAT?](#)

[P. ¿Es SNAT compatible con el ruteo asimétrico?](#)

## NAT-PT (v6 a v4)

[P. ¿Qué es la NAT-PT?](#)

[P. ¿Se admite la NAT-PT en la ruta de Cisco Express Forwarding \(CEF\)?](#)

---

[P. ¿Qué ALG se admiten en la NAT-PT?](#)

[P. ¿Los ASR 1004 admiten la NAT-PT?](#)

#### [Plataformas Cisco 7300/7600/6k](#)

[P. ¿La NAT con estado \(SNAT\) está disponible en Catalyst 6500 en la serie SX?](#)

[P. ¿En el hardware de 6k se admite la NAT consciente del VRF?](#)

[P. ¿Cat6000 y 7600 admiten la NAT consciente del VRF?](#)

#### [Plataforma Cisco 850](#)

[P. ¿Cisco 850 admite el ALG de la NAT de Skinny en la versión 12.4T?](#)

#### [Implementación de NAT](#)

[P. ¿Cómo se implementa la NAT?](#)

[P. ¿Cómo se implementa una NAT con voz?](#)

[P. ¿Cómo se integra la NAT con VPN de MPLS?](#)

[P. ¿La correspondencia estática de la NAT admite el protocolo HSRP para alta disponibilidad?](#)

[P. ¿Cómo implemento NAT NVI?](#)

[P. ¿Cómo se implementa el equilibrio de carga con la NAT?](#)

[P. ¿Cómo implemento NAT junto con IPSec?](#)

[P. ¿Cómo implemento la NAT-PT?](#)

[P. ¿Cómo se implementa la NAT multidifusión?](#)

[P. ¿Cómo se implementa la NAT con estado \(SNAT\)?](#)

#### [Mejores prácticas para NAT](#)

[P. ¿Existen mejores prácticas para la NAT?](#)

#### [Información Relacionada](#)

---

## Introducción

En este documento se brindan las respuestas para las preguntas frecuentes sobre la Traducción de direcciones de red (NAT).

## NAT genérica

P. ¿Qué significa "NAT"?

R. La traducción de direcciones de red (NAT) está diseñada para conservar direcciones IP. Permite que se conecten a Internet las redes de IP privada que emplean direcciones IP no registradas. NAT opera en routers, que en general conectan dos redes, y convierte las direcciones privadas (no exclusivas globalmente) de la red interna en direcciones legales, antes de que se reenvíen los paquetes a otra red.

Se puede configurar NAT para que difunda al mundo exterior solo una dirección para toda la red. Esto brinda más seguridad, al ocultar de hecho detrás de esa dirección toda la red interna. NAT ofrece la doble función de seguridad y conservación de direcciones, y suele implementarse en entornos de acceso remoto.

P. ¿Cómo funciona NAT?

R. Básicamente, permite que un dispositivo, como un router, haga de agente entre Internet (o la red pública) y una red local (o red privada), lo cual significa que solo se necesita una dirección IP exclusiva para representar a todo un grupo de computadoras fuera de una red.

P. ¿Cómo se configura NAT?

R. Para la configuración de la NAT tradicional, hay que crear al menos dos interfaces en un router (una es la NAT externa y otra la NAT interna) y un conjunto de reglas para la traducción de las direcciones IP de los encabezados (y las cargas útiles, si se desea) de los paquetes. Para configurar la interfaz virtual de NAT (NVI), necesita al menos una interfaz configurada con NAT activada y con el mismo conjunto de reglas antes mencionado.

Para obtener más información, consulte la [Guía de Configuración de IP Addressing Services de Cisco IOS®](#) o [Configuración de la Interfaz Virtual NAT](#).

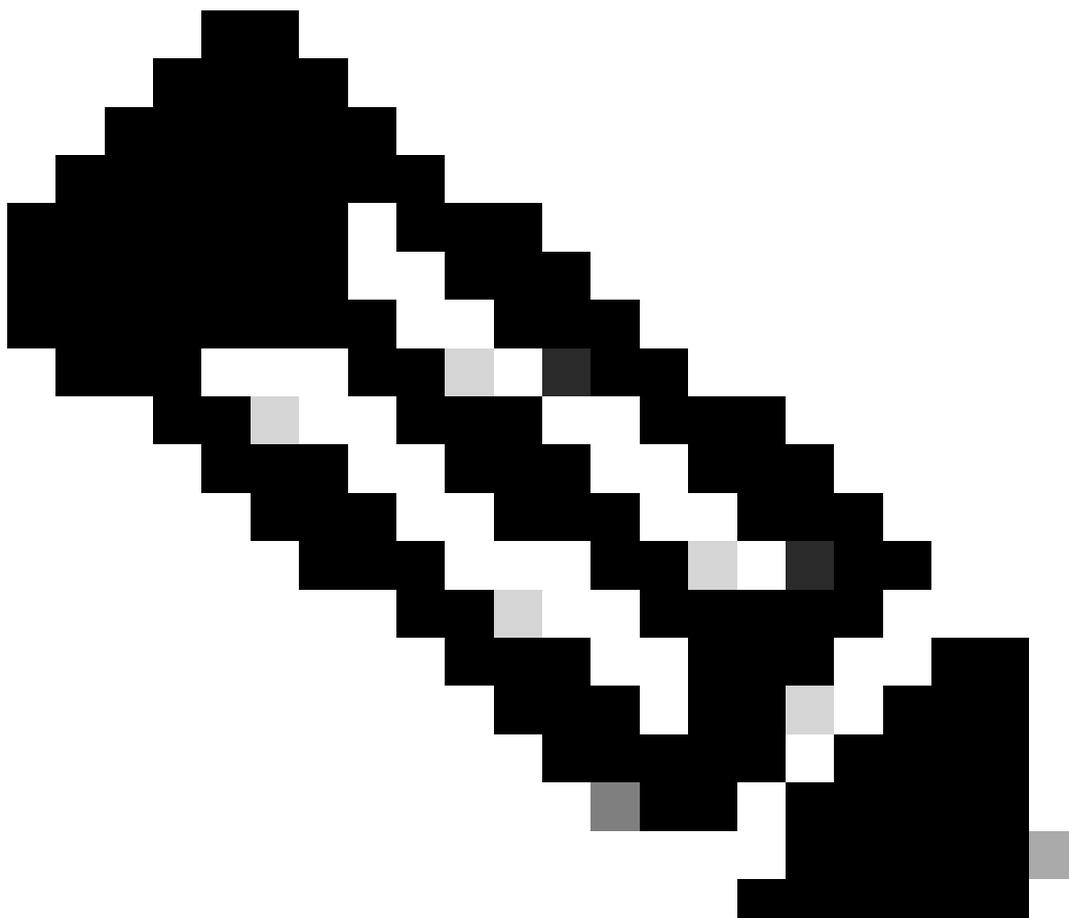
P. ¿Cuáles son las diferencias principales entre las implementaciones de NAT del Cisco IOS Software y Cisco PIX Security Appliance?

R. La NAT del software Cisco IOS no tiene grandes diferencias respecto de la función de NAT del dispositivo de seguridad Cisco PIX. Una de las principales tiene que ver con los diferentes tipos de tráfico admitidos por cada implementación. Consulte Ejemplos de configuración de la NAT para ver más información sobre la configuración de la NAT en los dispositivos Cisco PIX (incluye los tipos de tráfico admitidos).

P. ¿Con qué hardware de routing Cisco se ofrece NAT en Cisco IOS? ¿Cómo se puede comprar el hardware?

R. La herramienta Cisco Feature Navigator permite a los clientes identificar una función (NAT) y averiguar en qué versión de versión y hardware está disponible esta función del software Cisco IOS. Consulte Buscador de funciones de Cisco para ver cómo usar esta herramienta.

---



Nota: solo los usuarios registrados de Cisco pueden acceder a la información y las herramientas internas de Cisco.

---

P. ¿La NAT ocurre antes o después del ruteo?

R. El orden en que se procesan las transacciones con la NAT depende de si los paquetes van de la red interna a la red externa o de la red externa a la red interna. La traducción del interior al exterior se realiza tras el routing, mientras que la inversa se realiza antes. Consulte Orden de operación de NAT para ver más información.

P. ¿Se puede implementar NAT en un entorno de LAN inalámbrica pública?

R. Sí. La función de compatibilidad de NAT con direcciones IP estáticas permite que los usuarios de dichas direcciones establezcan una sesión IP en un entorno de LAN inalámbrica pública.

P. ¿NAT hace equilibrio de carga TCP para servidores en la red interna?

R. Sí. Con NAT, puede establecer un host virtual en la red interna que coordine la compartición de cargas entre hosts reales.

P. ¿Puedo limitar la cantidad de traducciones NAT?

R. Sí. La función de limitación de traducciones NAT permite establecer el máximo de operaciones de NAT simultáneas en un router. Además de brindar a los usuarios más control sobre el modo de uso de las direcciones de NAT, esta función se puede emplear para limitar los efectos de virus, gusanos y ataques de denegación de servicio.

P. ¿Cómo se aprende o propaga el routing en direcciones o subredes IP empleadas por NAT?

A. Se aprende el ruteo para las direcciones IP creadas por NAT si:

- El grupo de direcciones globales internas se obtiene de la subred de un router del siguiente salto.
- La entrada de ruta estática se configura en el router del siguiente salto y se redistribuye dentro de la red de routing.

Cuando la dirección global interna coincide con la interfaz local, NAT instala un alias IP y una entrada ARP, en cuyo caso el router puede proxy-arp para estas direcciones. Si no desea este comportamiento, use la palabra clave no-alias.

Al configurar un grupo de NAT, se puede usar la opción add-route para la inyección de rutas automática.

P. ¿Cuántas sesiones NAT simultáneas son admitidas en el NAT de Cisco IOS?

R. El límite de sesiones de NAT depende de la cantidad de DRAM disponible en el router. Cada traducción NAT consume alrededor de 312 bytes de DRAM. Por ende, 10 000 traducciones (más de lo habitual en un router) consumen alrededor de 3 MB. Es decir que el hardware de routing típico posee memoria más que suficiente para miles de traducciones NAT.

P. ¿Qué tipo de rendimiento de routing puede esperarse al usar la NAT de Cisco IOS?

R. La NAT de Cisco IOS ofrece switching de Cisco Express Forwarding, switching rápido y switching por proceso. En la versión 12.4T y las posteriores, ya no se ofrece la ruta de switching rápido. Para la plataforma Cat6k, el orden de switching es Netflow (ruta de switching de HW), CEF y ruta de proceso.

El rendimiento depende de varios factores:

- El tipo de aplicación y su tipo de tráfico
- Si las direcciones IP están integradas

- El intercambio y la inspección de varios mensajes
- El puerto de origen requerido
- La cantidad de traducciones
- Las otras aplicaciones que se ejecuten en el momento
- El tipo de hardware y de procesador

P. ¿La NAT de Cisco IOS puede aplicarse en subinterfaces?

R. Sí. Las traducciones NAT de origen o destino pueden aplicarse en cualquier interfaz o subinterfaz que tenga una dirección IP (incluso interfaces de marcadores). NAT no puede configurarse con la interfaz virtual inalámbrica. La interfaz virtual inalámbrica no existe al momento de escribir en NVRAM. Por ende, el router pierde la configuración de NAT en la interfaz virtual inalámbrica.

P. ¿La NAT de Cisco IOS puede usarse con el protocolo de router de reserva activa (HSRP) para ofrecer enlaces redundantes a un proveedor de servicios de Internet?

R. Sí. NAT ofrece redundancia de HSRP. Sin embargo, es diferente a la SNAT (NAT con estado). La NAT con HSRP es un sistema sin información de estado. La sesión actual no se mantiene ante las fallas. Durante la configuración de NAT estática (cuando un paquete no coincide con ninguna configuración de regla ESTÁTICA), el paquete se envía sin traducción.

P. ¿La NAT de Cisco IOS admite traducciones entrantes en una interfaz Frame Relay? ¿Es compatible con las traducciones de salida en el lado Ethernet?

R. Sí. El encapsulamiento no es relevante para NAT. Se puede emplear NAT cuando hay una dirección IP en una interfaz y la interfaz es de NAT interna o externa. Debe haber un interior y un exterior para que funcione NAT. Si emplea NVI, debe haber al menos una interfaz con NAT activada. Consulte [¿Cómo configuro NAT?](#) para obtener más detalles.

P. ¿Un router con NAT activada puede permitir que algunos usuarios empleen NAT y otros usuarios de la misma interfaz Ethernet continúen usando sus propias direcciones IP?

R. Sí. Esto se puede hacer mediante una lista de acceso donde se describan los grupos de hosts o redes que requieren NAT.

Para definir las reglas que determinan la traducción de los dispositivos IP, se pueden emplear listas de acceso, listas de acceso ampliadas y mapas de rutas. Siempre deben especificarse la dirección de red y la máscara de subred apropiada. La palabra clave any no se debe utilizar en lugar de la dirección de red o la máscara de subred. Con la NAT estática, cuando el paquete no coincide con ninguna configuración de regla ESTÁTICA, el paquete se envía sin ninguna traducción.

P. Al configurar para PAT (sobrecarga), ¿cuál es la cantidad máxima de traducciones que pueden crearse por dirección IP global interna?

A.PAT (sobrecarga) divide los puertos disponibles por dirección IP global en tres intervalos: 0-511, 512-1023 y 1024-65535. PAT asigna un puerto de origen exclusivo para cada sesión de TCP o UDP. Intenta asignar el mismo valor de puerto de la solicitud original, pero, si el puerto ya está ocupado, comienza a buscar desde el comienzo de ese rango de puertos hasta hallar uno disponible para asignarlo a la conversación. Existe una excepción para la base de códigos 12.2S. La base de códigos 12.2S emplea una lógica de puerto diferente y no ofrece reserva de puertos.

P. ¿Cómo funciona PAT?

R. La PAT trabaja con una dirección IP global o con varias direcciones.

PAT con una dirección IP

Condición	Descripción
1	NAT/PAT inspecciona el tráfico y lo evalúa según una regla de traducción.
2	La regla representa una configuración de PAT.
3	Si PAT conoce el tipo de tráfico y si ese tipo de tráfico tiene "un conjunto de puertos específicos o puertos que negocia" que utiliza, PAT los aparta y no los asigna como identificadores únicos.
4	Si una sesión sin requisitos de puertos especiales intenta conectarse con el exterior, PAT traduce la dirección IP de origen y verifica la disponibilidad del puerto de origen (433, por ejemplo).  Nota: Para el protocolo de control de transmisión (TCP) y el protocolo de datagramas de usuario (UDP), los intervalos son: 1-511, 512-1023, 1024-65535. Para el protocolo de mensajería de control de Internet (ICMP), el primer grupo comienza con el número 0.
5	Si el puerto de origen solicitado está disponible, PAT lo asigna y la sesión continúa.
6	Si no está disponible, PAT comienza a buscar desde el comienzo del mismo grupo (desde 1 para aplicaciones de UDP o TCP, y desde 0 para ICMP).
7	Al hallar un puerto disponible, lo asigna y la sesión continúa.
8	Si no hay puertos disponibles, el paquete se pierde.

PAT con varias direcciones IP

Condición	Descripción
1-7	Las primeras siete condiciones son las mismas que para cuando hay una sola dirección IP.
8	Si no hay puertos disponibles en el mismo grupo en la primera dirección IP, NAT pasa a la siguiente dirección IP del grupo e intenta asignar el puerto de origen solicitado.
9	Si el puerto de origen solicitado está disponible, NAT lo asigna y la sesión continúa.
10	Si no está disponible, NAT comienza a buscar desde el comienzo del mismo grupo

	(desde 1 para aplicaciones de UDP o TCP, y desde 0 para ICMP).
11	Si existe un puerto disponible, éste es asignado y la sesión prosigue.
12	Si no hay puertos disponibles, el paquete se rechaza, a menos que haya disponible otra dirección IP en el grupo.

## P. ¿Qué son los grupos de IP de NAT?

R. Los grupos de IP de la NAT son un rango de direcciones IP asignadas para NAT según sea necesario. Para definir un grupo, se emplea el comando de configuración:

<#root>

```
ip nat pool <name> <start-ip> <end-ip>
    {netmask <netmask> | prefix-length <prefix-length>}
    [type {rotary}]
```

### Ejemplo 1

El siguiente ejemplo traduce entre hosts internos dirigidos desde la red 192.168.1.0 o 192.168.2.0 a la red global única 10.69.233.208/28:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
ip address 10.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

### Ejemplo 2

En este ejemplo, el objetivo es definir una dirección virtual, cuyas conexiones se distribuyen entre un conjunto de hosts reales. El grupo define las direcciones de los hosts reales. La lista de acceso define la dirección virtual. Si aún no existe una traducción, los paquetes de TCP de la interfaz de serie 0 (la interfaz externa) cuyos destinos figuren en la lista de acceso se convierten en una dirección del grupo.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
```

```
ip address 192.168.15.129 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.15.17 255.255.255.240
ip nat inside
!
access-list 2 permit 192.168.15.1
```

P. ¿Cuál es el número máximo de agrupaciones IP de NAT configurables (ip nat pool <name>)?

R. En la práctica, la cantidad máxima de grupos de IP configurables depende de la cantidad de DRAM disponible en un router en particular. (Cisco recomienda configurar 255 grupos). Cada conjunto no debe tener más de 16 bits. En la versión 12.4(11)T y posteriores, Cisco IOS introduce CCE (Common Classification Engine). Esto marca un límite de 255 grupos para NAT. En la base de códigos 12.2S, no hay restricciones para la cantidad de grupos.

P. ¿Cuál es la ventaja de usar mapa de rutas en lugar de ACL en un grupo de NAT?

R. Un mapa de rutas impide que usuarios externos no deseados lleguen a los servidores/usuarios internos. También puede establecer una correspondencia entre una dirección IP interna y diferentes direcciones globales internas según la regla. Para ver más información, consulte [Uso de NAT con varios grupos mediante mapas de rutas](#).

P. ¿Qué es la superposición de direcciones IP en el contexto de NAT?

R. Se trata de una situación donde dos ubicaciones que quieren conectarse emplean el mismo esquema de direccionamiento IP. No se trata de algo inusual, sino que suele suceder cuando las empresas se fusionan o adquieren. Sin un soporte especial, las dos ubicaciones no pueden conectarse y establecer sesiones. La dirección IP superpuesta puede ser una dirección pública asignada a otra empresa, una dirección privada asignada a otra empresa o puede provenir del intervalo de direcciones privadas definido en [RFC 1918](#)

Las direcciones IP privadas no permiten routing y exigen traducciones NAT para permitir conexiones con el mundo exterior. La solución supone interceptar las respuestas de consultas de nombres del sistema de nombres de dominio (DNS) que van del exterior al interior, configurar una traducción para la dirección externa y preparar la respuesta de DNS antes de reenviar al host interno. Se necesita un servidor DNS de ambos lados del dispositivo de NAT para determinar qué usuarios quieren tener una conexión entre las dos redes.

NAT puede inspeccionar y traducir direcciones presentes en los registros de DNS A y PTR, como se indica en [Uso de NAT en redes superpuestas](#).

P. ¿Qué son las traducciones NAT estáticas?

R. Las NAT estáticas ofrecen correspondencia una a una entre direcciones locales y globales. Los usuarios también pueden configurar traducciones de direcciones estáticas en el nivel del puerto, y emplear el resto de la dirección IP para otras traducciones. Esto suele suceder al realizar traducciones de direcciones de puertos (PAT).

El siguiente ejemplo muestra cómo configurar el mapa de ruta para permitir la traducción de afuera hacia adentro para NAT estática:

```
<#root>
```

```
ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!  
ip access-list extended ACL-A  
permit ip any 10.1.10.128 0.0.0.127'  
  
route-map R1 permit 10  
match ip address ACL-A
```

P. ¿Qué se entiende por el término sobrecarga de NAT? ¿Es PAT?

R. Sí. La sobrecarga de NAT es PAT, que supone el uso de un grupo con un rango de una o más direcciones, o el uso de una dirección IP de interfaz en combinación con el puerto. Al sobrecargar, se crea una traducción totalmente ampliada. Se trata de una entrada de tabla de traducción que contiene la dirección IP y el puerto de origen/destino, y se suele denominar PAT o sobrecarga.

PAT (o sobrecarga) es una función de la NAT de Cisco IOS empleada para convertir direcciones privadas internas (locales internas) en una o más direcciones IP externas (globales internas, generalmente registradas). Para distinguir las conversaciones, se utilizan números de puerto de origen únicos en cada traducción.

P. ¿Qué son las traducciones NAT dinámicas?

R. En las NAT dinámicas, los usuarios pueden establecer una correspondencia dinámica entre direcciones locales y globales. La correspondencia dinámica se logra al definir las direcciones locales que se van a traducir y el grupo de direcciones o la dirección IP de interfaz desde donde se asignarán direcciones globales, y asociar las dos partes.

P. ¿Qué es ALG?

R. ALG significa gateway de capa de aplicación. NAT presta el servicio de traducción para todo tráfico de protocolo de control de transmisión/protocolo de datagramas de usuarios (TCP/UDP) que no lleve direcciones IP de origen o destino en el flujo de datos de aplicación.

Estos protocolos son FTP, HTTP, SKINNY, H232, DNS, RAS, SIP, TFTP, telnet, archie, finger, NTP, NFS, rlogin, rsh y rcp. Los protocolos específicos que integran información de direcciones IP en la carga útil deben admitir un gateway de nivel de aplicación (ALG).

Para ver más información, consulte [Uso de gateways de nivel de aplicación con NAT](#).

P. ¿Es posible crear una configuración con traducciones NAT estáticas y dinámicas?

R. Sí. Sin embargo, no se puede emplear la misma dirección IP para la configuración estática de NAT ni en el grupo para configuración dinámica de NAT. Todas las direcciones IP públicas deben ser exclusivas. Tenga en cuenta que las direcciones globales empleadas en traducciones estáticas no se excluyen automáticamente en los grupos dinámicos que contienen esas mismas direcciones globales. Deben crearse grupos dinámicos para excluir las direcciones asignadas a entradas estáticas. Para ver más información, consulte [Configuración de NAT estática y dinámica en simultáneo](#).

P. Cuando se realiza un traceroute a través de un router NAT, ¿traceroute muestra la dirección NAT-Global o filtra la dirección NAT-Local?

R. Traceroute desde el exterior siempre debe devolver la dirección global.

P. ¿Cómo asigna PAT los puertos?

R. NAT introduce características adicionales de puerto: rango completo y mapa de puerto.

- La primera permite que NAT use todos los puertos, más allá de su rango predeterminado.
- La segunda permite que NAT reserve un rango de puertos definido por el usuario para aplicaciones específicas.

Para ver más información, consulte [Rangos de puertos de origen definidos por el usuario para PAT](#).

Desde la versión 12.4(20)T2 en adelante, NAT presenta aleatorización de puertos para puertos simétricos y L3/L4.

- La aleatorización permite que NAT seleccione al azar cualquier puerto global para la solicitud de puerto de origen.
- El puerto simétrico permite que NAT admita independiente del punto de soporte.

P. ¿Cuál es la diferencia entre la fragmentación de IP y la segmentación de TCP?

R. La fragmentación de IP se produce en la capa 3 (IP); la segmentación de TCP se produce en la capa 4 (TCP). La fragmentación de IP sucede cuando desde una interfaz se envían paquetes más grandes que la unidad máxima de transmisión (MTU) de la interfaz. Estos paquetes deben fragmentarse o descartarse cuando se envían por la interfaz. Si el bit Do not Fragment (DF) no está configurado en el encabezado IP del paquete, el paquete se fragmenta. Si el bit DF está configurado en el encabezado IP del paquete, el paquete se descarta y se devuelve al remitente un mensaje de error ICMP que indica el valor de MTU de salto siguiente. Todos los fragmentos de

un paquete de IP llevan la misma identificación en el encabezado de IP, lo cual permite al receptor final armar con los fragmentos el paquete de IP original. Para ver más información, consulte [Resuelva problemas de fragmentación de IP, MTU, MSS y PMTUD con GRE e IPsec.](#)

La segmentación de TCP sucede cuando una aplicación de una estación final está enviando datos. Los datos de la aplicación se dividen en partes del tamaño que TCP considere ideal para el envío. Estas unidades de datos que pasan de TCP a IP se denominan segmentos. Los segmentos de TCP se envían en datagramas de IP. Estos datagramas de IP luego pueden convertirse en fragmentos de IP al avanzar por la red y encontrar enlaces de MTU más bajos de lo que necesitan para pasar.

TCP primero segmenta estos datos en segmentos TCP (según el valor TCP MSS) y agrega el encabezado TCP y pasa este segmento TCP a IP. Luego, el protocolo IP agrega un encabezado IP para enviar el paquete al host extremo remoto. Si el paquete IP con el segmento TCP es mayor que la MTU IP en una interfaz saliente en la trayectoria entre los hosts TCP, IP fragmenta el paquete IP/TCP para que encaje. La capa IP reensambla estos fragmentos de paquete IP en el host remoto y el segmento TCP completo (que se envió originalmente) se entrega a la capa TCP. La capa TCP no tiene idea de que IP ha fragmentado el paquete durante el tránsito. NAT admite fragmentos IP, pero no admite segmentos TCP.

P. ¿NAT admite fragmentación de IP y segmentación de TCP fuera de orden?

R. La NAT solo admite fragmentos de IP fuera de orden debido a ip virtual-reassembly.

P. ¿Cómo se depuran la fragmentación de IP y la segmentación de TCP?

R. NAT utiliza la misma CLI de depuración para la fragmentación de IP y la segmentación de TCP: debug ip nat frag.

P. ¿Hay alguna MIB de NAT compatible?

R. No. No hay ninguna MIB de NAT compatible, incluida CISCO-IETF-NAT-MIB.

P. ¿Qué es el tiempo de espera de TCP y cómo se relaciona con el temporizador de TCP de NAT?

R. Si el intercambio de señales de tres vías no se completa y NAT ve un paquete TCP, NAT inicia un temporizador de 60 segundos. Tras completarse el protocolo de enlace triple, NAT emplea de forma predeterminada un temporizador de 24 horas para una entrada de NAT. Si un host final envía un RESET, NAT cambia el temporizador predeterminado de 24 horas a 60 segundos. En el caso de FIN, NAT cambia el temporizador predeterminado de 24 horas a 60 segundos cuando recibe FIN y FIN-ACK.

P. ¿Puedo cambiar la cantidad de tiempo que tarda una traducción NAT en agotar el tiempo de espera de la tabla de traducción NAT?

R. Sí. Puede cambiar los valores de tiempo de espera de NAT para todas las entradas o para

diferentes tipos de traducciones de NAT (como udp-timeout, dns-timeout, tcp-timeout, finrst-timeout, icmp-timeout, pptp-timeout, syn-timeout, port-timeout y arp-ping-timeout).

P. ¿Cómo impido que el protocolo ligero de acceso a directorios (LDAP) adjunte bytes de más en cada paquete de respuesta de LDAP?

R. La configuración del protocolo LDAP suma los bytes adicionales (resultados de búsquedas del protocolo LDAP) cuando procesa mensajes del tipo Search-Res-Entry. LDAP adjunta 10 bytes de resultados de búsquedas en cada paquete de respuesta de LDAP. Si por estos 10 bytes adicionales el paquete supera la unidad máxima de transmisión (MTU) de una red, el paquete se rechaza. En ese caso, Cisco recomienda desactivar este comportamiento de LDAP mediante el comando de CLI `no ip nat service append-ldap-search-res` para que los paquetes se puedan enviar y recibir.

P. ¿Cuál es la ruta recomendada para la dirección IP global interna/local externa en la caja de NAT?

R. En la caja de NAT configurada debe especificarse una ruta para la dirección IP global interna para funciones tales como NAT-NVI. De manera similar, también se debe especificar una ruta en el cuadro NAT para la dirección IP local externa. En este caso, cualquier paquete de una dirección de entrada a salida que utilice la regla estática externa requiere este tipo de ruta. En tales escenarios, al tiempo que se proporciona la ruta para IG/OL, también se debe configurar la dirección IP del salto siguiente. Si falta la configuración del siguiente salto, esto se considera un error de configuración y da como resultado un comportamiento indefinido.

NVI-NAT solo está presente en la ruta de la función de salida. Si tiene una subred conectada directamente con NAT-NVI o tiene la regla de traducción NAT externa configurada en la caja, en esos escenarios debe indicar una dirección IP del siguiente salto falsa y también un ARP asociado para el siguiente salto. Esto es necesario para que la infraestructura subyacente entregue el paquete a NAT para la traducción.

P. ¿NAT de Cisco IOS soporta ACL con una palabra clave de registro?

R. Al configurar la NAT de Cisco IOS como NAT dinámica, se emplea una ACL para identificar los paquetes que pueden traducirse. La arquitectura NAT actual no admite ACL con una palabra clave log.

## NAT de voz

P. ¿La NAT admite Skinny Client Control Protocol (SCCP) v17 que viene con Cisco Unified Communications Manager (CUCM) V7?

R. CUCM 7 y todas las cargas telefónicas predeterminadas para CUCM 7 admiten SCCPv17. La versión de SCCP empleada es la versión más reciente que tengan tanto CUCM como el teléfono al registrarse el teléfono.

En el momento en que se creó este documento, NAT todavía no es compatible con SCCP v17. Hasta que se implemente el soporte NAT para SCCP v17, el firmware se debe degradar a la versión 8-3-5 o anterior para que se negocie SCCP v16. CUCM6 no encuentra el problema de NAT con ninguna carga telefónica, siempre y cuando utilice SCCP v16. Cisco IOS no admite por el momento la versión 17 de SCCP.

P. ¿Qué versiones de carga de CUCM/SCCP/firmware admite NAT?

R. La NAT admite las versiones de CUCM 6.x y anteriores. Estas versiones de CUCM se lanzan con la carga de firmware telefónico predeterminada 8.3.x (o anteriores) que admite SCCP v15 (o anteriores).

NAT no admite las versiones de CUCM 7.x o posteriores. Estas versiones de CUCM se lanzan con la carga de firmware telefónico predeterminada 8.4.x que admite SCCP v17 (o posteriores).

Si se emplea CUCM 7.x o posteriores, debe instalarse una carga de firmware anterior en el servidor TFTP de CUCM, para que los teléfonos usen una carga de firmware con SCCP v15 o anterior y sean compatibles con NAT.

P. ¿Qué es la mejora de asignación de puertos de PAT de proveedores de servicios para RTP y RTCP?

R. La función de mejora de asignación de puertos de la PAT de proveedores de servicios para los protocolos RTP y RTCP garantiza que para las llamadas de voz de Skinny, H.323 y SIP: Los números de puerto empleados para flujos RTP sean pares, mientras que para los flujos RTCP sean el siguiente número impar. El número de puerto se convierte en un número dentro del rango especificado en conformidad con RFC-1889. Una llamada con un número de puerto dentro del rango da como resultado una traducción PAT a otro número de puerto dentro de este rango. Del mismo modo, una traducción PAT para un número de puerto fuera de este rango no resulta en una traducción a un número dentro del rango dado.

P. ¿Qué es el protocolo SIP (Session Initiation Protocol)? ¿Se puede usar NAT con paquetes de SIP?

R. El protocolo de inicio de sesión (SIP) es un protocolo de control de capa de aplicación ASCII que puede utilizarse para establecer, mantener y terminar llamadas entre dos o más terminales. Fue desarrollado por el Grupo de Trabajo de Ingeniería de Internet (IETF) para conferencias multimedia por IP. La implementación de SIP de Cisco permite que las plataformas Cisco compatibles envíen la configuración de llamadas de voz y multimedia por redes IP.

Se puede usar NAT con los paquetes SIP.

P. ¿Qué es la compatibilidad de NAT transversal en host con controladores de límites de sesión (SBC)?

R. Esta función de Cisco IOS permite que un router de gateway de nivel de aplicación (ALG) del protocolo SIP de la NAT de Cisco IOS funcione como SBC en un gateway IP a IP multiservicio de

Cisco, lo cual contribuye a la buena transmisión de los servicios de voz por IP (VoIP).

Para ver más información, consulte [Configuración de la NAT transversal en host de Cisco IOS para controladores de límites de sesión.](#)

P. ¿Cuántas llamadas de SIP, Skinny y H323 admiten la CPU y la memoria de router con NAT?

R. La cantidad de llamadas admitidas por el router de NAT depende de la cantidad de memoria disponible en la caja y el poder de procesamiento de la CPU.

P. ¿Un router NAT soporta la segmentación TCP de paquetes Skinny y H323?

R. Cisco IOS-NAT soporta la segmentación TCP para H323 en la línea principal 12.4 y la segmentación TCP para SKINNY a partir de 12.4(6)T.

P. ¿Hay que prestar atención a algo al emplear una configuración de sobrecarga de NAT en una implementación de voz?

R. Sí. En esos casos, necesita el mensaje de registro para hacer NAT y crear una asociación de afuera hacia adentro a fin de llegar a este dispositivo interno. El dispositivo interno envía este registro de forma periódica y actualiza por NAT este puerto desprotegido/esta asociación a partir de la información del mensaje de la señal.

P. ¿Se conocen problemas causados por el empleo del comando `clear ip nat trans *` o `clear ip nat trans forced` en implementaciones de voz?

R. En las implementaciones de voz cuando ejecuta un comando `clear ip nat trans *` o un comando `clear ip nat trans forced` y tiene NAT dinámica, borra el agujero de clavija/asociación y debe esperar el siguiente ciclo de registro desde el dispositivo interno para restablecer esto. Cisco recomienda no utilizar estos comandos en las implementaciones de voz.

P. ¿NAT admite la solución de coubicación de voz?

R. No. Por el momento no se admite la solución de coubicación. La siguiente implementación con NAT (en el mismo equipo) se considera una solución de ubicación compartida: CME/DSP-Farm/SCCP/H323.

P. ¿NVI admite ALG de Skinny, de H323 o de TCP SIP?

R. No. Tenga en cuenta que el ALG del protocolo UDP SIP (empleado en la mayoría de las implementaciones) no se ve afectado.

## NAT con VRF/MPLS

P. ¿Un router NAT soporta alguna vez NATting en el mismo espacio de dirección

en un VRF al mismo tiempo que NATted en un espacio de dirección global?  
Actualmente, recibo esta advertencia: "% similar static entry (10.1.1.1 —> 10.210.2.2) already exists" cuando intento configurar esto:

```
<#root>
```

```
72UUT(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2
```

```
72UUT(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED
```

R. La NAT heredada soporta la configuración de dirección superpuesta sobre diferentes VRFs. Debería configurar la superposición por regla con la opción match-in-vrf y configurar ip nat inside/outside en el mismo VRF para tráfico de ese VRF específico. La compatibilidad con superposición no incluye la tabla de routing global.

Debe agregar la palabra clave match-in-vrf para las entradas de NAT estática de VRF superpuestas para diferentes VRF. Sin embargo, no se puede superponer direcciones de NAT de vrf y globales.

```
<#root>
```

```
72UUT(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED match-in-vrf
```

```
72UUT(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2 vrf BLUE match-in-vrf
```

P. ¿Las NAT antiguas admiten VRF-Lite (NAT de un VRF a otro VRF)?

R. No. Para eso hay que utilizar la NVI. Puede utilizar NAT heredada para hacer NAT de VRF a global o NAT dentro del mismo VRF.

## NAT NVI

P. ¿Qué es NAT NVI?

R. NVI es la sigla en inglés de "interfaz virtual de NAT". Permite que NAT traduzca entre dos VRF. Esta solución debe utilizarse en lugar de la traducción de direcciones de red en un solo

dispositivo.

P. ¿Se debe utilizar NAT NVI al realizar NAT entre una interfaz en global y una interfaz en un VRF?

R. Cisco recomienda usar la NAT heredada para la NAT global de VRF (ip nat inside/out) y entre interfaces del mismo VRF. NVI se usa para NAT entre diferentes VRF.

P. ¿Se admite segmentación de TCP para NAT-NVI?

R. No se admite la segmentación del protocolo TCP para NAT-NVI.

P. ¿NVI admite ALG de Skinny, de H323 o de TCP SIP?

R. No. Tenga en cuenta que el ALG del protocolo UDP SIP (empleado en la mayoría de las implementaciones) no se ve afectado.

P. ¿Se admite segmentación de TCP con SNAT?

R. La SNAT no admite ningún ALG del protocolo TCP (como SIP, SKINNY, H323 o DNS). Por ende, no se admite la segmentación de TCP. Pero sí se admiten UDP SIP y DNS.

## SNAT

P. ¿Qué es la NAT con estado (SNAT)?

R. La SNAT permite que dos o más traductores de direcciones de redes funcionen como un grupo de traducción. Un miembro del grupo se encarga de tráfico que exige la traducción de la información de direcciones IP. Además, informa al traductor de respaldo sobre los flujos activos en el momento. El traductor de respaldo luego puede usar dicha información para preparar duplicados de las entradas de la tabla de traducción. Por ende, si el traductor activo se ve afectado por una falla crítica, el tráfico se puede pasar rápidamente al traductor de respaldo. El flujo de tráfico continúa porque se usan las mismas traducciones de direcciones de redes y ya se había definido el estado de las traducciones.

P. ¿Se admite segmentación de TCP con SNAT?

R. La SNAT no admite ningún ALG del protocolo TCP (como SIP, SKINNY, H323 o DNS). Por ende, no se admite la segmentación de TCP. Pero sí se admiten UDP SIP y DNS.

P. ¿Es SNAT compatible con el routing asimétrico?

R. El ruteo asimétrico soporta NAT habilitando como colocación en cola. De forma predeterminada, las colas están activadas. Sin embargo, de 12.4(24)T en adelante, no se admiten las colas. Los clientes deben asegurarse de que los paquetes se envíen correctamente y de que se agregue la demora adecuada para que el routing asimétrico funcione bien.

## NAT-PT (v6 a v4)

P. ¿Qué es la NAT-PT?

R. La NAT-PT es la traducción de v4 a v6 para la NAT. La traducción de protocolo (NAT-PT) es un mecanismo de traducción IPv6-IPv4, como se define en [RFC 2765](#) y [RFC 2766](#), que permite que los dispositivos solo IPv6 se comuniquen con dispositivos solo IPv4 y viceversa.

P. ¿Se admite NAT-PT en la ruta de Cisco Express Forwarding (CEF)?

R. No, no se admite la NAT-PT en la ruta de CEF.

P. ¿Qué ALG se admiten en NAT-PT?

R. La NAT-PT admite los protocolos TFTP/FTP y el DNS. No se admite voz ni SNAT en NAT-PT.

P. ¿Los ASR 1004 admiten NAT-PT?

R. Los routers de servicios de agregación (ASR) emplean NAT64.

## Plataformas Cisco 7300/7600/6k

P. ¿La NAT con estado (SNAT) está disponible en Catalyst 6500 en la serie SX?

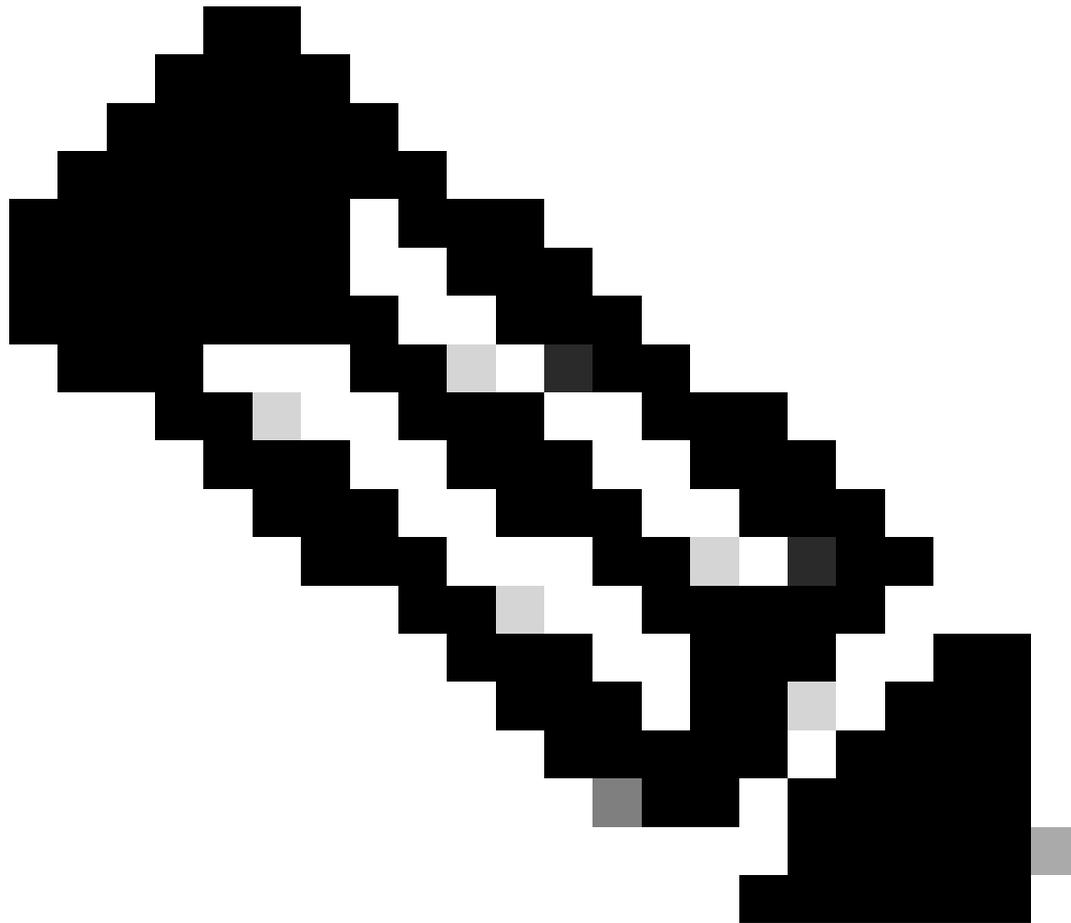
R. La SNAT no está disponible en Catalyst 6500 en la serie SX.

P. ¿En el hardware de 6k se admite NAT conciente de VRF?

R. No se admite la NAT conciente del VRF en el hardware de esta plataforma.

P. ¿7600 y Cat6000 admiten NAT conciente de VRF?

R. En la plataforma 65xx/76xx no se admite la NAT conciente del VRF y se bloquean las CLI.



Nota: Puede implementar un diseño empleando un FWSM que funcione en modo de contexto virtual transparente.

---

## Plataforma Cisco 850

P. ¿Cisco 850 admite el ALG de la NAT de Skinny en la versión 12.4T?

R. No. No se admite el ALG en la NAT de Skinny en la versión 12.4T en la serie 850.

## Implementación de NAT

P. ¿Cómo se implementa la NAT?

A. NAT habilita redes IP privadas entre sí que utilizan direcciones IP no registradas para conectarse a Internet. NAT convierte la dirección privada (RFC1918) de la red interna en direcciones que permiten routing de forma legal antes del reenvío de los paquetes a otra red.

P. ¿Cómo se implementa NAT con voz?

R. La función de compatibilidad de NAT con voz permite que los mensajes integrados en el protocolo SIP que pasan por un router configurado con NAT se vuelvan a convertir en un paquete. Se emplea un gateway de capa de aplicación (ALG) con NAT para traducir los paquetes de voz.

P. ¿Cómo se integra NAT con VPN de MPLS?

R. Esta función de integración permite configurar varias VPN de MPLS en un mismo dispositivo para que funcionen en conjunto. NAT puede distinguir de qué VPN recibe el tráfico IP aunque todas usen el mismo esquema de direccionamiento IP. Esta mejora permite que varios clientes de VPN de MPLS compartan servicios y garantiza que todas las VPN estén totalmente separadas entre sí.

P. ¿La correspondencia estática de NAT admite HSRP para alta disponibilidad?

R. Cuando se dispara una consulta de protocolo de resolución de direcciones (ARP) para una dirección configurada con correspondencia estática de NAT y perteneciente al router, la NAT responde con la dirección MAC de BIA en la interfaz que apunta el protocolo ARP. Dos routers hacen de HSRP activo y en espera. Sus interfaces de NAT interna deben estar activadas y configuradas para pertenecer a un grupo.

P. ¿Cómo se implementa NAT NVI?

R. La interfaz virtual de NAT (NVI) hace innecesario configurar una interfaz como de NAT interna o externa.

P. ¿Cómo se implementa el equilibrio de carga con NAT?

R. Hay dos tipos de balanceo de carga que se pueden hacer con NAT: puede equilibrar la carga entrante a un conjunto de servidores para distribuir la carga en los servidores, y puede equilibrar la carga del tráfico de usuario a Internet a través de dos o más ISP.

Para obtener más información sobre el balanceo de carga saliente, consulte [Balanceo de Carga NAT de Cisco IOS para Dos Conexiones ISP](#).

P. ¿Cómo se implementa NAT junto con IPSec?

R. Existe compatibilidad con la carga útil de seguridad de encapsulamiento (ESP) de seguridad IP (IPSec) mediante la NAT y compatibilidad con la transparencia de la NAT de IPSec.

La función de ESP de IPSec mediante NAT permite admitir varios túneles o conexiones de ESP de IPSec simultáneos, mediante un dispositivo de NAT de Cisco IOS configurado en el modo de sobrecarga o traducción de direcciones de puertos (PAT).

La función de transparencia de NAT de IPSec ofrece compatibilidad para que el tráfico de IPSec pase por puntos de NAT o PAT de la red ocupándose de las incompatibilidades conocidas entre

NAT e IPsec.

P. ¿Cómo se implementa NAT-PT?

R. NAT-PT (traducción de direcciones de red: traducción de protocolo) es un mecanismo de traducción IPv6-IPv4, como se define en [RFC 2765](#) y [RFC 2766](#), que permite que los dispositivos sólo IPv6 se comuniquen con dispositivos sólo IPv4 y viceversa.

P. ¿Cómo se implementa NAT multidifusión?

R. Se puede hacer una NAT de IP de origen de flujos multidifusión. No se puede usar mapas de rutas al hacer NAT dinámica para multidifusión; para esto solo se admiten listas de acceso.

Para ver más información, consulte Cómo funciona NAT multidifusión en los routers Cisco. En los grupos multidifusión de destino se hace NAT mediante una solución de reflejo de servicio multidifusión.

P. ¿Cómo se implementa NAT con estado (SNAT)?

R. La SNAT ofrece servicio continuo para sesiones de NAT de correspondencia dinámica. Las sesiones de definición estática reciben el beneficio de la redundancia sin necesidad de SNAT. Ante la ausencia de SNAT, las sesiones que emplean correspondencias de NAT dinámica finalizarían en caso de una falla crítica y deberían restablecerse. Solo se admite la configuración de SNAT mínima. Las implementaciones futuras solo se deben realizar después de hablar con el equipo de cuentas de Cisco para validar el diseño en relación con las restricciones actuales.

SNAT se recomienda para los siguientes escenarios:

- El modo principal/respaldo no se recomienda, ya que le faltan algunas funciones que sí tiene HSRP.
- Para escenarios de conmutación por falla y para configuraciones de 2 routers. Es decir, si falla un router, el otro se hace cargo de inmediato (la arquitectura de SNAT no está diseñada para manejar flapeo de interfaces).
- Se admite el escenario de routing no asimétrico. El routing asimétrico solo se puede hacer si la latencia en el paquete de respuesta es superior a la existente entre 2 routers SNAT para intercambiar los mensajes de SNAT.

Actualmente, la arquitectura SNAT no está diseñada para administrar la robustez; por lo tanto, no se espera que estas pruebas tengan éxito:

- Eliminación de entradas de NAT mientras hay tráfico.
- Cambio de los parámetros de la interfaz (como el cambio de la dirección IP, el cierre/no cierre, etc.) mientras hay tráfico.
- No se espera que los comandos específicos de SNAT clear o show se ejecuten bien; no se

recomiendan.

Algunos de los comandos relacionados con SNAT `clear` y `show` son los siguientes:

```
<#root>
clear ip snat sessions *
clear ip snat sessions <ip address of the peer>
clear ip snat translation distributed *
clear ip snat translation peer < IP address of SNAT peer>
sh ip snat distributed verbose
sh ip snat peer < IP address of peer>
```

- Si el usuario desea borrar entradas, se pueden utilizar los comandos `clear ip nat trans forced` o `clear ip nat trans *`.
- Si el usuario desea ver las entradas, se pueden utilizar los comandos `show ip nat translation`, `show ip nat translations verbose` y `show ip nat stats`. Si se configura `service internal`, también muestra información específica de SNAT.
- No se recomienda eliminar traducciones NAT en el router de respaldo. Siempre elimine las entradas de NAT en el router SNAT principal.
- SNAT no es HA; por lo tanto, las configuraciones en ambos routers deben ser las mismas. Ambos routers deben tener la misma imagen en ejecución. También asegúrese de que la plataforma subyacente empleada para los dos routers SNAT sea la misma.

## Mejores prácticas para NAT

P. ¿Existen mejores prácticas para la NAT?

R. Sí. Estas son las mejores prácticas para NAT:

1. Al utilizar NAT dinámica y estática, la ACL que establece la regla para NAT dinámica debe excluir los hosts locales estáticos para que no se superpongan.
2. Trate de no usar ACL para NAT con `permit ip any any`, porque los resultados pueden ser imprevisibles. Después de 12.4(20)T, NAT traduce los paquetes de protocolo de ruteo y HSRP generados localmente si se envían fuera de la interfaz externa, así como los paquetes cifrados localmente que coinciden con la regla NAT.
3. Cuando tenga redes superpuestas para NAT, use la palabra clave `match-in-vrf`.

Debe agregar la palabra clave `match-in-vrf` en las entradas de NAT estática de VRF superpuestas para diferentes VRF, pero no se puede superponer direcciones de NAT de vrf

y globales.

```
<#root>
```

```
Router(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED match-in-vrf
```

```
<#root>
```

```
Router(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2 vrf BLUE match-in-vrf
```

4. Los grupos de NAT con el mismo rango de direcciones no pueden usarse en VRF diferentes, a menos que se emplee la palabra clave match-in-vrf.

Por ejemplo:

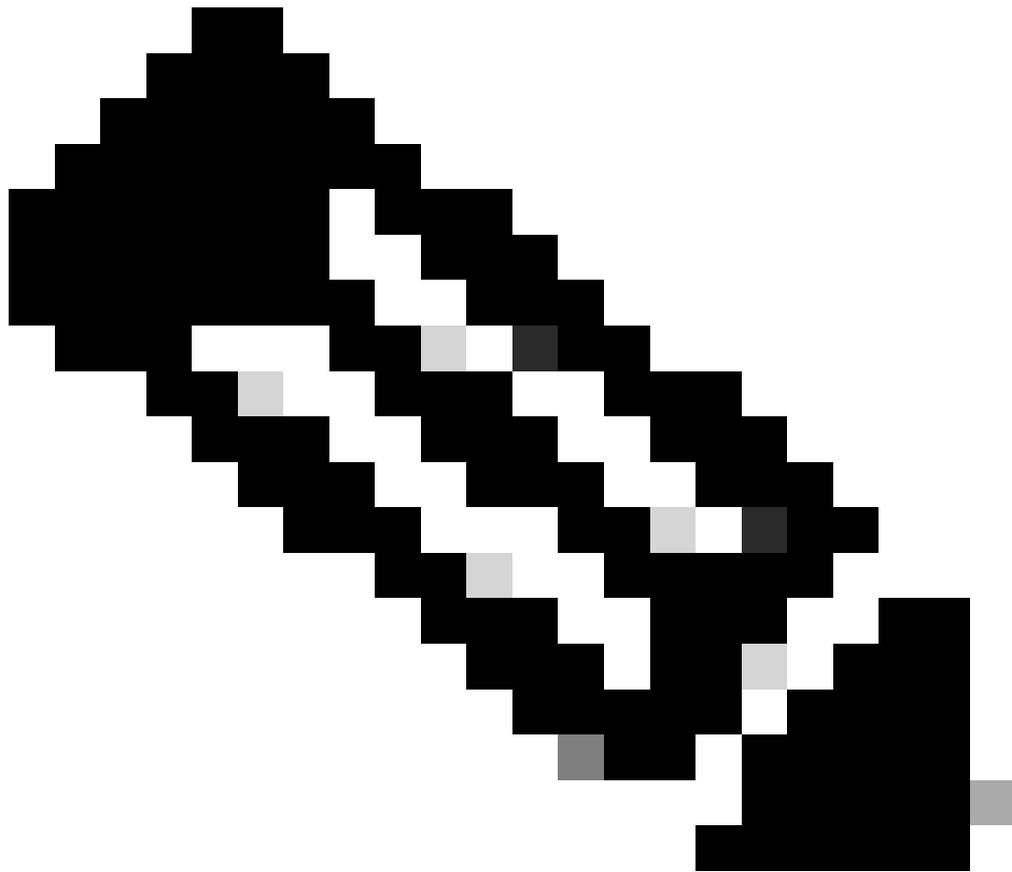
```
<#root>
```

```
ip nat pool poolA 1710.1.1.1 1710.1.1.10 prefix-length 24
```

```
ip nat pool poolB 1710.1.1.1 1710.1.1.10 prefix-length 24
```

```
ip nat inside source list 1 poolA vrf A match-in-vrf
```

```
ip nat inside source list 2 poolB vrf B match-in-vrf
```



Nota: Aunque la configuración de CLI es válida, sin la palabra clave match-in-vrf la configuración no es compatible.

- 
5. Al implementar equilibrio de carga de proveedores de servicios de Internet con sobrecarga de interfaz de NAT, la mejor práctica es usar un mapa de rutas con coincidencia en interfaz en lugar de coincidencia en ACL.
  6. Al utilizar la asignación de grupo, no debe utilizar dos asignaciones diferentes (ACL o route-map) para compartir la misma dirección de grupo NAT.
  7. Al implementar las mismas reglas NAT en dos routers diferentes en el escenario de failover, debe utilizar la redundancia HSRP.
  8. No defina una misma dirección global interna en NAT estática y en un grupo dinámico. Esto puede generar resultados no deseados.

## Información Relacionada

- [Soporte técnico y descargas de Cisco](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).