Preguntas frecuentes sobre la traducción de direcciones de red (NAT)

Contenido

Introducción

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

NAT genérica

Q. ¿Qué es NAT?

A. 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.

Q. ¿Cómo funciona NAT?

A. Básicamente, permite que un dispositivo, como un router, haga de agente entre la Internet (o 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 su red.

Q. ¿Cómo se configura NAT?

A. Para la configuración de 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 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 ver más información, consulte Guía de configuración de servicios de direcciones IP de Cisco IOS o Configuración de la interfaz virtual de NAT.

Q. ¿Cuáles son las diferencias principales entre las implementaciones de NAT del software Cisco IOS® y del dispositivo de seguridad Cisco PIX?

A. La NAT del software Cisco IOS no tiene grandes diferencias con 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 Dispositivos de seguridad de la serie Cisco PIX 500 y Ejemplos de configuraciones de NAT para ver más información sobre la configuración de NAT en dispositivos Cisco PIX (se incluyen los tipos de tráfico admitidos).

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

A. El buscador de funciones de Cisco permite a los clientes identificar funciones (NAT) y ver en qué versiones de hardware y software Cisco IOS se ofrecen. Consulte Buscador de funciones de Cisco para ver cómo usar esta herramienta.

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

A. El orden en que se procesan las transacciones con NAT depende de si los paquetes van de la red interna hacia la red externa o al revés. 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.

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

A. Yes. 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.

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

A. Yes. Con NAT, puede establecer un host virtual en la red interna que coordine la compartición de cargas entre hosts reales. Para ver más información, consulte Evite la sobrecarga de servidores mediante el equilibrio de carga TCP.

Q. ¿Puedo limitar la cantidad de traducciones NAT?

A. Yes. 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.

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

A. El routing de las direcciones IP creadas por NAT se aprende 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 de IP y una entrada de ARP, en cuyo caso el router emplea **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.

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

A. El límite de sesiones NAT depende de la 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.

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

A. 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

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

A. Yes. 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.

Q. ¿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?

A. Yes. 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.

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

A. Yes. 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 se configura NAT? para ver más detalles.

Q. ¿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?

A. Yes. Esto se puede hacer mediante una lista de acceso donde se describan los grupos de hosts o redes que requieren NAT. Todas las sesiones del mismo host se traducirán o pasarán por el router sin traducción.

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 correspondiente máscara de subred. No debe usarse la palabra clave **any** en lugar de la dirección de red o máscara de subred (para ver más detalles, consulte Preguntas frecuentes, mejores prácticas y guía de implementación de NAT). Con la configuración de NAT estática, cuando un paquete no coincide con ninguna configuración de regla ESTÁTICA se lo hace pasar sin traducción.

Q. 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 rangos: 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.

Q. ¿Cómo funciona PAT?

A. 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 ese tipo de tráfico tiene "un grupo de puertos específicos o puertos que negocia" para utilizar, PAT los separa y no los asigna como identificadores exclusivos.
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 UDP, los rangos son: 1-511, 512-1023 y 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.

Q. ¿Qué son los grupos de IP de NAT?

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

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

Ejemplo 1

En el siguiente ejemplo se traduce de hosts internos de la red 192.168.1.0 o 192.168.2.0 a la red exclusiva a nivel global 10.69.233.208/28:

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

Ejemplo 2

En el siguiente ejemplo, la meta es definir una dirección virtual, cuyas conexiones entrantes se distribuyan entre un grupo 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 <name> <start-ip> <end-ip> {netmask <netmask> | prefix-length <prefix-length>} [type {rotary}]
```

Q. ¿Cuál es la cantidad máxima de grupos de IP de NAT configurables ("nombre" de ip nat pool)?

A. En la práctica, la cantidad máxima depende de la cantidad de DRAM disponible en el router (Cisco recomienda configurar 255 grupos). Cada grupo no debe superar los 16 bits. En la versión 12.4(11)T y las posteriores, IOS suma CCE (motor de clasificación común). Esto marca un límite de 255 grupos para NAT. En la base de códigos 12.2S, no hay restricciones para la cantidad de grupos.

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

A. 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.

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

A. Se trata de una situación donde dos ubicaciones que quieren conectarse emplean el mismo esquema de direccionamiento IP. Esto no es inusual; suele suceder al fusionar o adquirir empresas. Sin soporte especial, las dos ubicaciones no podrán conectarse y establecer sesiones. La dirección IP superpuesta puede ser una dirección pública asignada a otra empresa, ser una dirección privada asignada a otra empresa, o provenir del rango 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.

Q. ¿Qué son las traducciones NAT estáticas?

A. Las traducciones NAT estáticas ofrecen correspondencia uno a uno 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).

En el siguiente ejemplo se muestra cómo configurar el mapa de rutas para permitir la traducción del exterior al interior para NAT estática:

```
ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 30.1.10.128 0.0.0.127'
route-map R1 permit 10
match ip address ACL-A
```

Q. ¿Qué se entiende por el término sobrecarga de NAT? ¿Se trata de PAT?

A. Yes. 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.

Q. ¿Qué son las traducciones NAT dinámicas?

A. En estas traducciones, 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.

Q. ¿Qué es ALG?

A. ALG es un gateway de capas 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.

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

A. Yes. 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.

Q. ¿Al hacer un traceroute mediante un router NAT, el traceroute debería mostrar la dirección global de NAT o revelar la dirección local de NAT?

A. Un traceroute desde el exterior siempre debería regresar la dirección global.

Q. ¿Cómo asigna PAT los puertos?

A. NAT introduce más funciones para puertos: rango completo y mapa de puertos.

- 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.
- Con puertos simétricos, NAT puede admitir la opción *independiente de las terminales*.

Para ver más información, consulte Anatomía: Una mirada dentro de los traductores de direcciones de redes.

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

A. La fragmentación de IP sucede en la capa 3 (IP), Mientras que la segmentación de TCP se da 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 al enviarse desde la interfaz. Si en el encabezado de IP del paquete no se configuró el bit de no fragmentar (DF), el paquete se fragmenta. Si en el encabezado IP del paquete figura el bit de DF, el paquete se rechaza y un mensaje de error de ICMP indica que el valor de MTU del siguiente salto se regresará al remitente. 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 divide estos datos en segmentos de TCP (según el valor de MSS de TCP), agrega el encabezado de TCP y pasa este segmento a IP. Luego IP agrega un encabezado de IP para enviar el paquete al host final remoto. Si el paquete de IP con el segmento de TCP es más grande que la MTU de IP en una interfaz saliente de la ruta entre los hosts de TCP, IP fragmenta el paquete de IP/TCP para que quepa. La capa IP junta estos fragmentos del paquete de IP en el host remoto y luego el segmento de TCP completo (enviado originalmente) se envía a la capa de TCP. La capa de TCP no tiene idea de que IP había fragmentado el paquete en tránsito.

NAT admite fragmentos de IP, pero no admite segmentos de TCP.

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

A. NAT solo admite fragmentos de IP fuera de orden debido a **ip virtual-reassembly**.

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

A. NAT emplea la misma CLI de depuración para ambos: **debug ip nat frag**.

Q. ¿Hay alguna MIB de NAT compatible?

A. No. No hay MIB de NAT compatibles; CISCO-IETF-NAT-MIB no es compatible.

Q. ¿Qué es el *tiempo de espera de TCP* y cómo se relaciona con el temporizador

de TCP de NAT?

A. Si el protocolo de enlace triple no se completó y NAT ve un paquete de 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.

Q. ¿Puedo cambiar el tiempo de espera de las traducciones NAT desde la tabla de traducciones NAT?

A. Yes. Puede cambiar los valores de tiempo de espera de NAT de todas las entradas o de diferentes tipos de traducciones NAT (como udp-timeout, dns-timeout, tcp-timeout, finrst-timeout, icmp-timeout, pptp-timeout, syn-timeout, port-timeout y arp-ping-timeout).

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

A. La configuración de LDAP suma los bytes adicionales (resultados de búsquedas de LDAP) al procesar 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.

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

A. En la caja de NAT configurada debe especificarse una ruta para la dirección IP global interna para funciones como NAT-NVI. De la misma manera, debe especificarse una ruta en la caja de NAT para la dirección IP local externa. En este caso, todos los paquetes en dirección del interior al exterior que empleen la regla estática externa necesitan este tipo de ruta. En dichos escenarios, al indicar la ruta para la dirección IP global interna/local externa, también debe configurarse la dirección IP del siguiente salto. Si no hay configuración del siguiente salto, se considera que hay un error de configuración y se genera 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.

Q. ¿La NAT de Cisco IOS admite ACL con la palabra clave "log"?

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

NAT de voz

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

A. 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.

NAT aún no admite SCCP v17. Hasta que NAT admita SCCP v17, el firmware debe regresarse a la versión 8-3-5 o las anteriores para emplear SCCP v16. CUCM6 no hallará el problema de NAT con ninguna carga telefónica siempre y cuando emplee SCCP v16. Cisco IOS no admite por el momento la versión 17 de SCCP.

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

A. NAT admite las versiones de CUCM 6.x y las 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.

En el siguiente enlace se confirma que la carga de firmware 8.3.x contiene SCCP v15 o anteriores y funciona con NAT, y que la carga de firmware 8.4.x contiene SCCP v17 y NO funciona con NAT.

http://third-gen-phones.gforge.cisco.com/twiki/prod/bin/view/Thirdgenphones/CCMLoadNumberAndCodeNameDecoderRing

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

A. La función de mejora de asignación de puertos de PAT de proveedores de servicios para 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 convierta en un número dentro del rango especificado en conformidad con RFC-1889. Las llamadas con números de puerto dentro del rango pasen a tener otro número dentro de este rango mediante una traducción PAT. La traducción PAT de los números de puerto fuera de este rango no genera un número dentro del rango.

Para ver más información, consulte Mejora de asignación de puertos de PAT de proveedores de servicios para RTP y RTCP.

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

A. Se trata de 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.

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

A. Esta función de Cisco IOS permite que un router de gateway de nivel de aplicación (ALG) de SIP de NAT de Cisco IOS funcione como SBC en un gateway IP a IP multiservicio Cisco, lo cual contribuye a la buena transmisión de los servicios de voz por IP (VoIP).

Para ver más información, consulte Configuración de NAT transversal en host de Cisco IOS para controladores de límites de sesión y NAT transversal en host de SP para llamadas de SIP mediante un controlador de límites de sesión de Cisco IOS.

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

A. La cantidad depende de la memoria disponible en la caja y el poder de procesamiento de la CPU.

Q. ¿Los routers NAT admiten segmentación de TCP en paquetes de Skinny y H323?

A. La NAT de IOS admite segmentación de TCP para H323 en 12.4 Mainline y para SKINNY de 12.4(6)T en adelante.

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

A. Yes. 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.

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

A. En las implementaciones de voz, al emplear el comando **clear ip nat trans ? o clear ip nat trans forced** y tener NAT dinámica, se borra el puerto desprotegido/la asociación y hay que esperar al siguiente ciclo de registro del dispositivo interno para restablecer esto. Cisco recomienda no utilizar estos comandos en las implementaciones de voz.

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

A. No. Por el momento no se admite. Se considera que la siguiente implementación con NAT (en la misma caja) es una solución de coubicación: CME/DSP-Farm/SCCP/H323.

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

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

NAT con VRF/MPLS

Q. ¿En algún momento los routers NAT van a admitir que se use NAT para convertir un mismo espacio de direcciones en un espacio de direcciones global y VRF? Actualmente, recibo esta advertencia: *"%"% similar static entry (1.1.1.1 ---> 22.2.2.2) already exists"* cuando intento configurar lo siguiente:

```
72UUT(config)#ip nat inside
 source static 1.1.1.1 22.2.2.2 72UUT(config)#ip nat inside source static
 1.1.1.1 22.2.2.2 vrf RED
```

A. Las NAT antiguas admiten la configuración de direcciones superpuestas en diferentes VRF. 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 superpuestos para diferentes VRF. Sin embargo, no se puede superponer direcciones de NAT de vrf y globales.

```
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf
```

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

A. No. Para esto hay que utilizar NVI. Puede usar NAT antiguas para hacer NAT de VRF a global o hacer NAT dentro del mismo VRF.

NAT NVI

Q. ¿Qué es NAT NVI?

A. NVI es la sigla en inglés para "interfaz virtual de NAT". Permite que NAT traduzca entre dos VRF. Debería usarse esta solución en lugar de traducción de direcciones de redes en una sola interfaz física.

Q. ¿Debe usarse NAT NVI para NAT entre una interfaz de global y una interfaz de VRF?

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

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

A. No se admite.

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

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

Q. ¿Se admite segmentación de TCP con SNAT?

A. SNAT no admite ningún ALG de 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

Q. ¿Qué es la NAT con estado (SNAT)?

A. 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. Para ver más información, consulte Más recuperabilidad de IP mediante la NAT con estado de Cisco.

Q. ¿Se admite segmentación de TCP con SNAT?

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

Q. ¿Se admite SNAT para el routing asimétrico?

A. El routing asimétrico admite NAT al activar las colas. 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)

Q. ¿Qué es NAT-PT?

A. NAT-PT es la traducción de v4 a v6 para NAT. La traducción de protocolos (NAT-PT) es un mecanismo de traducción IPv6-IPv4 según la definición en RFC 2765 y RFC 2766 , que permite a los dispositivos de solo IPv6 comunicarse con los de solo IPv4 y viceversa. Para ver más información sobre esta función, consulte Implementación de NAT-PT para IPv6

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

A. No, no se admite.

Q. ¿Qué ALG se admiten en NAT-PT?

A. NAT-PT admite TFTP/FTP y DNS. No se admite voz ni SNAT en NAT-PT.

Q. ¿Los ASR 1004 admiten NAT-PT?

A. Los routers de servicios de agregación (ASR) emplean NAT64. Para ver más información sobre la configuración de NAT64, consulte Configuración de una red de routing para NAT64 sin estado.

Plataformas Cisco 7300/7600/6k

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

A. No está disponible.

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

A. No se admite en el hardware de esta plataforma.

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

A. En la plataforma 65xx/76xx no se admite NAT conciente de 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

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

A. No. No se admite en la serie 850.

Implementación de NAT

Q. ¿Cómo se implementa NAT?

A. NAT permite que se conecten a Internet las redes de IP privada que emplean direcciones IP no registradas. 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.

Para ver más información sobre la implementación de NAT, consulte Configuración de NAT para la conservación de direcciones IP.

Q. ¿Cómo se implementa NAT con voz?

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

Para ver más información sobre la implementación de NAT con voz, consulte Compatibilidad de NAT con ALG.

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

A. 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.

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

A. 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, NAT responde con la dirección MAC de BIA en la interfaz donde apunta el 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.

Q. ¿Cómo se implementa NAT NVI?

A. La interfaz virtual de NAT (NVI) hace innecesario configurar una interfaz como de NAT interna o externa. Para ver más información sobre NAT NVI, consulte Configuración de la interfaz virtual de NAT.

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

A. Existen dos tipos de equilibrio de carga que pueden emplearse con NAT: se puede equilibrar la carga entrante de un grupo de servidores para distribuirla, o bien, se puede equilibrar la carga de tráfico a Internet de los usuarios con dos o más proveedores de servicios.

Para ver más información sobre el equilibrio de carga entrante, consulte Evite la sobrecarga de servidores mediante el equilibrio de carga TCP.

Para ver más información sobre el equilibrio de carga saliente, consulte Equilibrio de carga de NAT de IOS para conexiones de dos proveedores de servicios de Internet.

Q. ¿Cómo se implementa NAT en conjunto con IPSec?

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

Q. ¿Cómo se implementa NAT-PT?

A. NAT-PT (Traducción de direcciones de redes - Traducción de protocolos) es un mecanismo de traducción IPv6-IPv4 según la definición de RFC 2765 y RFC 2766 , que permite a los dispositivos de solo IPv6 comunicarse con los de solo IPv4 y viceversa.

Para ver más información sobre la implementación y la configuración de NAP-PT, consulte Implementación de NAT-PT para IPv6.

Q. ¿Cómo se implementa NAT multidifusión?

A. Se puede hacer NAT de la 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.

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

A. 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. Antes de llevar a cabo implementaciones en el futuro, debería hablar con el equipo de su cuenta de Cisco para validar el diseño en relación con las restricciones actuales.

Se recomienda SNAT para los siguientes escenarios:

- El modo HSRP tal como se describe en el informe técnico sobre SNAT: Más recuperabilidad de IP mediante la NAT con estado de Cisco.
- 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.

Por el momento, la arquitectura de SNAT no está diseñada para aceptar robustez; por ende, no se espera que estas pruebas sean exitosas:

- Eliminación de entradas de NAT mientras hay tráfico.
- Cambio de parámetros de interfaces (como cambio de direcciones IP, apagar/no apagar, etc.)

mientras hay tráfico.
- No se espera que los comandos específicos de SNAT **clear** o **show** se ejecuten bien; no se recomiendan.Estos son algunos de los comandos relativos a SNAT **clear** y **show**:

```
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 eliminar entradas, se puede usar los comandos **clear ip nat trans forced** o **clear ip nat trans ?.**Si el usuario desea ver entradas, se puede usar los comandos **show ip nat translation**, **show ip nat translations verbose** y **show ip nat stats**. Si se configura el *servicio interno*, también mostrará información 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 ende, las configuraciones en los dos routers deberían ser iguales. Los dos routers deberían ejecutar la misma imagen. También asegúrese de que la plataforma subyacente empleada para los dos routers SNAT sea la misma.

Mejores prácticas para NAT

Q. ¿Existen mejores prácticas para NAT?

A. Yes. Estas son las mejores prácticas para NAT:

1. Al utilizar NAT dinámica y estática, la ACL que define la regla para NAT dinámica debería excluir los hosts locales estáticos a fin de que no haya superposición.
2. Trate de no usar ACL para NAT con **permit ip any any**, porque los resultados pueden ser imprevisibles. A partir de 12.4(20)T, NAT traduce paquetes de protocolo de routing y HSRP generados de manera local si se envían fuera de la interfaz externa, y también los paquetes encriptados de manera local que coincidan con la regla de 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.
   ```
   Router(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf


   Router(config)#ip nat inside source static 1.1.1.1 22.2.2.2 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:

   ```
   ip nat pool poolA 171.1.1.1 171.1.1.10 prefix-length 24
   ip nat pool poolB 171.1.1.1 171.1.1.10 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 sea válida, la configuración no se admite sin la palabra clave **match-in-vrf**.

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 correspondencias de grupos, no debería usar dos correspondencias diferentes (ACL o mapa de rutas) para compartir la misma dirección de grupo de NAT.
7. Al implementar las mismas reglas de NAT en dos routers diferentes en el escenario de conmutación por falla, debería usar redundancia de 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

- Compatibilidad con tecnología de routing IP
- Soporte Técnico y Documentación - Cisco Systems