

Cómo evitar loops de ruteo al utilizar la NAT dinámica

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Convenciones](#)

[Situación de ejemplo](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe un escenario en el cual los paquetes coloquen entre el router NAT y el router de la venciencia en la interfaz exterior al usar la traducción de dirección de red dinámica (NAT) debida traficar destinado para un IP Address inusitado en un agrupamiento NAT y la presencia de una ruta predeterminado en el router NAT que rutea estos paquetes de nuevo al exterior.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

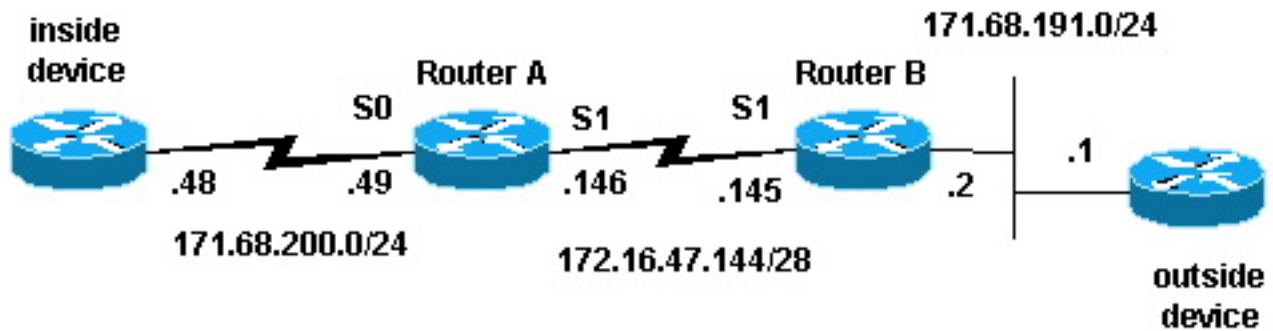
[Componentes Utilizados](#)

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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

[Diagrama de la red](#)

La topología siguiente fue utilizada para crear el ejemplo de escenario.



Convenciones

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

Situación de ejemplo

En la topología antedicha, el Router A se configura con el NAT de modo que traduzca los paquetes originados de la red 171.68.200.0/24 a un rango de direcciones definido por el agrupamiento NAT “test-loop”. La configuración Router-a es como sigue (configuran al resto del Routers con las Static rutas para obtener la Conectividad):

```
hostname Router-A
!
!
ip nat pool test-loop 172.16.47.161 172.16.47.165 prefix-length 28
ip nat inside source list 7 pool test-loop
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 no ip mroute-cache
 no ip route-cache
 no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside
 no ip mroute-cache
 no ip route-cache
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
access-list 7 permit 171.68.200.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
```

```
login
!  
end
```

Con los comandos de depuración de paquetes IP y de depuración de traducción NAT, generamos un ping desde el router en el dispositivo interno. El ping trabajado, y una entrada de la tabla de traducción fueron generados. En el siguiente resultado, vemos que la depuración de paquetes IP y la depuración IP NAT se encuentran activas y que no hay entradas en la tabla de traducción por el momento.

Nota: Los comandos **debug** generan una cantidad significativa de resultados. Utilícelos sólo cuando el tráfico en la red del IP es lento, con el fin de que no se vea afectada negativamente otra actividad del sistema.

```
Router-A# show debug Generic IP: IP packet debugging is on (detailed) IP NAT debugging is on  
Router-A# show ip nat translations Router-A#
```

El router interno (dispositivo interno) origina un paquete ICMP con una dirección de origen de 171.68.200.48 y una dirección de destino de 171.68.191.1 (la dirección del dispositivo externo). **La salida de los debugs** siguiente muestra un paquete del IP con una dirección IP de origen de 171.68.200.48 que es traducida a 172.16.47.161. El paquete ingresa en la interfaz Serial0 y tiene como destino salir de la interfaz Serial1.

```
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [401]  
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0
```

La siguiente salida de depuración muestra el paquete IP de retorno con una dirección IP de destino 172.16.47.161 que se vuelve a traducir a 171.68.200.48. El paquete viene en la interfaz del Serial1 y se destina hacia fuera la interfaz del serial0.

```
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [401]  
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=0, code=0
```

El resultado de la depuración muestra el intercambio de ping exitoso entre el dispositivo interno y el dispositivo externo:

```
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [402]  
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0  
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [402]  
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=0, code=0  
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [403]  
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0  
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [403]  
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=0, code=0  
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [404]  
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0  
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [404]  
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=0, code=0  
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [405]  
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0  
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [405]  
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=0, code=0
```

Al usar el comando `show ip nat translations` se puede ver una entrada en la tabla de traducción correspondiente al dispositivo interno.

```
Router-A# show ip nat translations Pro Inside global Inside local Outside local Outside global -  
-- 172.16.47.161 171.68.200.48 --- ---
```

Ahora que existe una traducción para el dispositivo interno en la tabla de traducción, podemos realizar un ping exitoso desde el dispositivo externo a la dirección global del dispositivo interno, como se muestra a continuación en la salida de los depuradores generada por el Router-A.

Nota: La dirección de origen del paquete que el dispositivo externo originó es 171.68.191.1 y su dirección de destino es 172.16.47.161 (la dirección global interna en la tabla de traducción).

```
Router-A#  
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [108]  
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=8, code=0  
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [108]  
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=0, code=0  
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [109]  
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=8, code=0  
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [109]  
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=0, code=0  
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [110]  
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=8, code=0  
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [110]  
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=0, code=0  
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [111]  
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=8, code=0  
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [111]  
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=0, code=0  
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [112]  
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=8, code=0  
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [112]  
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=0, code=0
```

La salida de los debugs siguiente demuestra qué puede suceder cuando un dispositivo externo intenta iniciar la comunicación con una dirección destino que sea una dirección IP inusitada en la agrupación de Test-Loop. Utilizaron al **comando clear ip nat translation** de borrar la tabla de traducción y un ping fue enviado a una dirección IP inusitada dentro de la agrupación de Test-Loop.

El dispositivo externo envía un paquete ICMP destinado para la dirección global interna de 172.16.47.161. Sin embargo, la interfaz de salida es lo mismo que la interfaz de entrada para este paquete.

```
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0  
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0  
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0
```

```
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
ICMP type=8, code=0
```

NAT traduce los paquetes que van desde afuera hacia adentro antes de su ruteo. En este caso, no hay entrada en la tabla de traducción, así que el Router A puede rutear solamente el paquete. El Router A confía en su ruta predeterminado para rutear los paquetes, enviando los paquetes se retira la interfaz del Serial1, que causa un loop que podría derribar eventual la línea serial.

Para evitar este tipo de loop de ruteo, no origine los paquetes desde dispositivos externos a las direcciones globales internas. Sin embargo, como esto es difícil de lograr, puede agregar una ruta estática para las direcciones globales internas con un salto siguiente de null0 en el Router A. De esta manera, cuando un dispositivo externo envía paquetes destinados a una dirección global interna, y no existe ninguna entrada en la tabla de conversión, el router A enruta el paquete a null0, evitando el loop. Si se toma el ejemplo anterior, la ruta estática es similar a lo siguiente:

```
ip route 172.16.47.160 255.255.255.252 null0.
```

[Información Relacionada](#)

- [Página de Soporte de NAT](#)
- [Página de Soporte de IP Routed Protocols](#)
- [Página de Soporte de IP Routing](#)
- [Soporte Técnico - Cisco Systems](#)