

Éviter les boucles de routage en mode NAT dynamique

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Diagramme du réseau](#)

[Conventions](#)

[Exemple de scénario](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit un scénario dans lequel des paquets circulent en boucle entre le routeur NAT et le routeur voisin sur l'interface externe lors de l'utilisation de la traduction d'adresses de réseau dynamique (NAT) en raison du trafic destiné à une adresse IP inutilisée dans un pool NAT et de la présence d'une route par défaut sur le routeur NAT qui achemine ces paquets vers l'extérieur.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

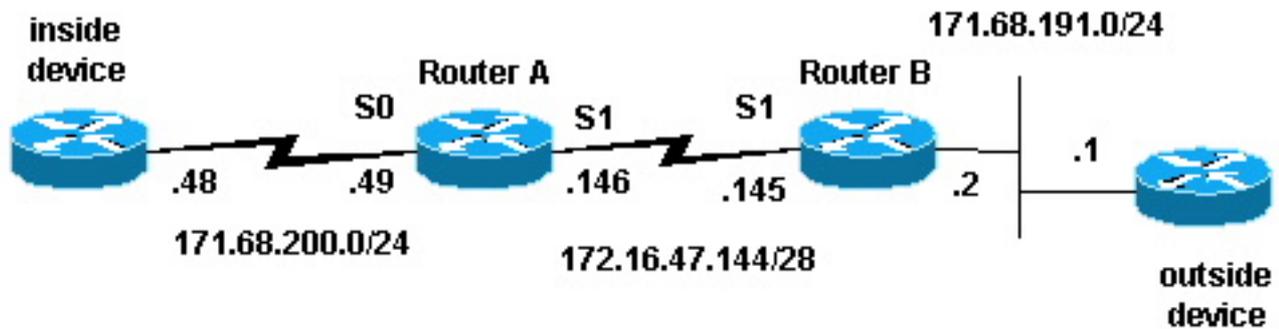
[Components Used](#)

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

[Diagramme du réseau](#)

La topologie suivante a été utilisée pour créer l'exemple de scénario.



Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

Exemple de scénario

Dans la topologie ci-dessus, le routeur A est configuré avec NAT de sorte qu'il traduit les paquets provenant du réseau 171.68.200.0/24 en une plage d'adresses définie par le pool NAT « test-loop ». La configuration du routeur A est la suivante (tous les autres routeurs sont configurés avec des routes statiques afin d'obtenir la connectivité) :

```
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
```

À l'aide des commandes NAT translation debugging et IP packet debugging, nous avons généré une requête ping à partir du routeur sur le périphérique interne. La requête ping a fonctionné et une entrée de table de traduction a été générée. Dans le résultat ci-dessous, nous voyons que le débogage de paquet IP et le débogage NAT IP sont activés et qu'il n'y a aucune entrée dans la table de traduction pour le moment.

Remarque : Les commandes **debug** génèrent une quantité significative de sortie. Utilisez-les seulement quand le trafic sur le réseau IP est faible, afin que le reste de l'activité sur le système ne soit pas affectée.

```
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#
```

Le routeur interne (périphérique interne) émet un paquet ICMP avec l'adresse source 171.68.200.48 et l'adresse de destination 171.68.191.1 (adresse du périphérique externe). La sortie de débogage suivante montre un paquet IP avec une adresse IP source de 171.68.200.48 traduite en 172.16.47.161. Le paquet arrive dans l'interface Serial0 et est destiné à l'interface 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 sortie de débogage suivante montre le paquet IP de retour avec une adresse IP de destination 172.16.47.161 traduite en 171.68.200.48. Le paquet arrive dans l'interface Serial1 et est destiné à l'interface 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
```

La sortie **debug** montre l'échange ping réussi entre le périphérique interne et le périphérique externe :

```
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

```

À l'aide de la commande **show ip nat translations**, nous voyons une entrée dans la table de traduction du périphérique interne.

```

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

```

Maintenant qu'une traduction pour le périphérique interne existe dans la table de traduction, nous pouvons envoyer une requête ping de l'équipement externe à l'adresse globale du périphérique interne, comme indiqué dans le résultat du débogage généré par le routeur A ci-dessous.

Remarque : Le paquet provenant du périphérique externe a l'adresse source 171.68.191.1 et l'adresse de destination 172.16.47.161 (l'adresse globale interne dans la table de traduction).

```

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

```

Le résultat de débogage suivant montre ce qui peut se produire lorsqu'un périphérique externe tente d'initier une communication avec une adresse de destination qui est une adresse IP inutilisée dans le pool de boucles de test. La commande **clear ip nat translation** a été utilisée pour effacer la table de traduction et une requête ping a été envoyée à une adresse IP inutilisée dans le pool de boucles de test.

Le périphérique externe envoie un paquet ICMP destiné à l'adresse globale interne 172.16.47.161. Cependant, l'interface de sortie est identique à l'interface d'entrée de ce paquet.

```
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
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 traduit les paquets de l'extérieur vers l'intérieur avant de les acheminer. Dans ce cas, il n'y a aucune entrée dans la table de traduction, de sorte que le routeur A peut seulement acheminer le paquet. Le routeur A utilise sa route par défaut pour acheminer les paquets, renvoyant les paquets à l'interface Serial1, ce qui entraîne une boucle qui pourrait éventuellement faire tomber la ligne série.

Pour éviter ce type de boucle de routage, ne lancez jamais de paquets des périphériques externes vers les adresses globales internes. Cependant, comme cela est difficile à appliquer, vous pouvez ajouter une route statique pour les adresses globales internes avec un saut suivant null0 dans le routeur A. De cette manière, lorsqu'un périphérique externe envoie des paquets destinés à une adresse globale interne et qu'il n'y a aucune entrée dans la table de traduction, le routeur A achemine le paquet vers null0, évitant ainsi la boucle. À l'aide de l'exemple ci-dessus, la route statique ressemble à ceci :

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

[Informations connexes](#)

- [Page de support NAT](#)
- [Page d'assistance pour les protocoles de routage IP](#)
- [Page de support pour le routage IP](#)
- [Support technique - Cisco Systems](#)