

Vérification et dépannage de la connectivité NAT de base

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Problème](#)

[Envoyez une requête ping à un routeur mais pas à un autre](#)

[Dépannage](#)

[Les périphériques externes au réseau ne peuvent pas communiquer avec les routeurs internes](#)

[Dépannage](#)

[Liste de vérification des problèmes courants](#)

[Traduction non installée dans la table de traduction](#)

[La saisie de traduction correcte n'est pas utilisée](#)

[NAT fonctionne correctement, mais il reste des problèmes de connectivité](#)

[%NAT System Busy - Essayer ultérieurement](#)

[La grande table de traduction augmente la CPU](#)

[Aucune entrée dans la table ARP](#)

[Informations connexes](#)

Introduction

Ce document décrit comment résoudre des problèmes de connectivité IP dans un environnement NAT et comment effectuer un dépannage.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Problème

Ce document décrit comment résoudre les problèmes de connectivité IP dans un environnement NAT en examinant les deux exemples suivants :

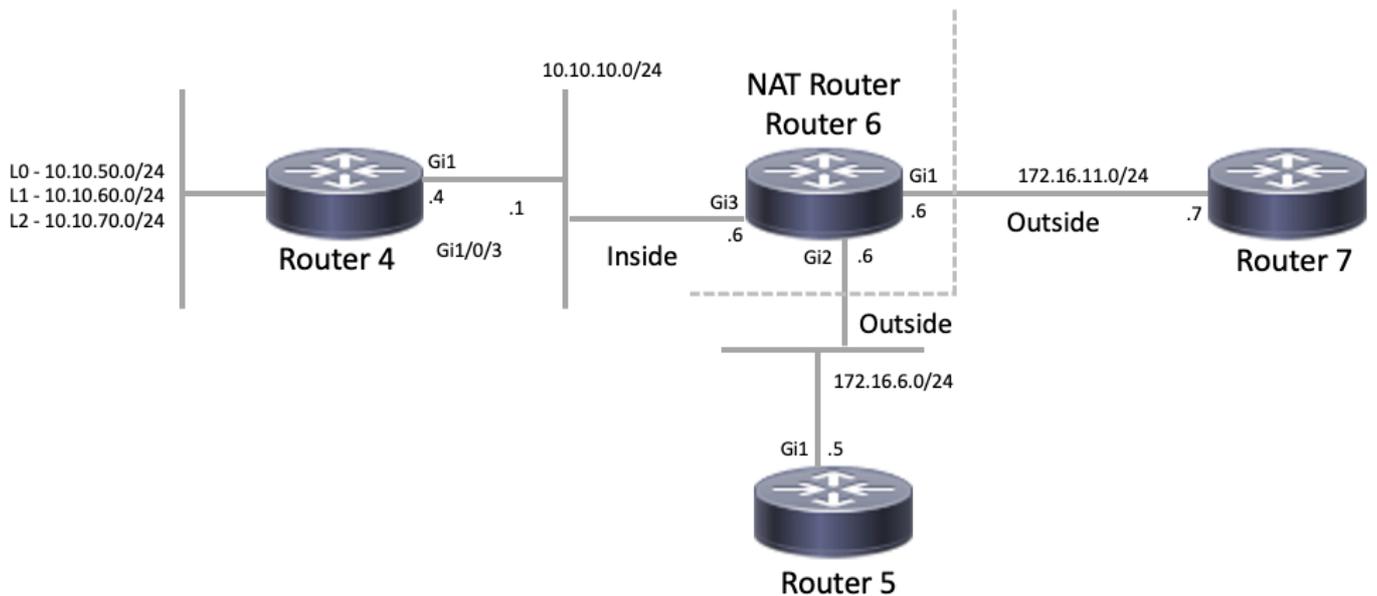
- Envoyez une requête ping à un routeur mais pas à un autre
- Les périphériques externes au réseau ne peuvent pas communiquer avec les routeurs internes

Les étapes de base suivantes sont utiles pour déterminer s'il y a un problème dans les opérations NAT :

1. Vérifiez la configuration et définissez clairement ce que la fonction NAT est censée réaliser. En vous basant sur l'examen, vous pouvez déterminer s'il y a un problème avec la configuration. Pour plus d'informations sur la configuration NAT, référez-vous à [Configurer la traduction d'adresses réseau](#).
2. Vérifiez que les traductions correctes existent dans la table de traduction.
3. Utilisez les commandes show et debug pour vérifier que la traduction se produit.
4. Examinez en détail ce qui arrive au paquet et vérifiez que les routeurs disposent des informations de routage correctes pour transférer le paquet.

Envoyez une requête ping à un routeur mais pas à un autre

Dans ce premier scénario, le routeur 4 peut envoyer une requête ping au routeur 5 (172.16.6.5), mais pas au routeur 7 (172.16.11.7) :



Topologie NAT

<#root>

Router4#

ping 172.16.6.5

Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 172.16.6.5, timeout is 2 seconds:
 .!!!!
 Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
 Router4#

ping 172.16.11.7

Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:

 Success rate is 0 percent (0/5)
 Router4#

Considérations importantes concernant ce scénario :

- Aucun protocole de routage dynamique n'est configuré sur les routeurs, seules les routes statiques sont utilisées.
- La passerelle par défaut du routeur 4 est le routeur 6.
- Le routeur 6 est configuré avec la NAT.

<#root>

```
interface GigabitEthernet1
ip address 172.16.11.6 255.255.255.0
```

```
ip nat outside
```

```

negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet2
ip address 172.16.6.6 255.255.255.0

ip nat outside

negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet3
ip address 10.10.10.6 255.255.255.0

ip nat inside

negotiation auto
no mop enabled
no mop sysid
!
!
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24 ip nat inside source static 10.10.10.4 172.16.11.70
!
ip access-list standard 7
10 permit 10.10.50.4
20 permit 10.10.60.4
30 permit 10.10.70.4

```

Dépannage

1. Tout d'abord, vous devez déterminer que la fonction NAT fonctionne correctement. À partir de la configuration précédente, il est possible de déterminer que l'adresse IP 10.10.10.4 du routeur 4 est traduite de manière statique en 172.16.6.14. Vous pouvez utiliser la commande `show ip nat translation` sur le routeur 6 pour vérifier que la traduction existe dans la table de traduction :

```
<#root>
```

```
NAT-Router#
```

```
show ip nat translations
```

```

Pro  Inside global      Inside local      Outside local      Outside global
---  172.16.6.14          10.10.10.4        ---                ---
Total number of translations: 1

```

```
NAT-Router#
```

2. Assurez-vous que cette traduction se produit lorsque le routeur 4 envoie du trafic IP. Vous

pouvez faire ceci de deux manières à partir du routeur 6 . Exécutez une commande NAT debug ou monitor NAT statistics avec la commande show ip nat statistics. Comme les commandes debug sont le dernier recours, commencez par la commande show.

3. Surveillez le compteur pour vous assurer qu'il augmente à mesure qu'il reçoit le trafic du routeur
4. Le compteur s'incrémente chaque fois que la table de traduction est utilisée pour traduire une adresse.

4. Effacez les statistiques, affichez-les, puis essayez d'envoyer une requête ping au routeur 7 à partir du routeur 4, puis affichez à nouveau les statistiques.

```
<#root>
```

```
NAT-Router#
```

```
clear ip nat statistics
```

```
NAT-Router#
```

```
NAT-Router#
```

```
show ip nat statistics
```

```
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
```

```
Outside interfaces:
```

```
  GigabitEthernet1, GigabitEthernet2
```

```
Inside interfaces:
```

```
  GigabitEthernet3
```

```
Hits: 0 Misses: 0
```

```
Expired translations: 0
```

```
Dynamic mappings:
```

```
-- Inside Source
```

```
[Id: 1] access-list 7 pool test refcount 0
```

```
  pool test: id 1, netmask 255.255.255.0
```

```
    start 172.16.11.70 end 172.16.11.71
```

```
    type generic, total addresses 2, allocated 0 (0%), misses 0
```

```
nat-limit statistics:
```

```
  max entry: max allowed 0, used 0, missed 0
```

```
In-to-out drops: 0 Out-to-in drops: 0
```

```
Pool stats drop: 0 Mapping stats drop: 0
```

```
Port block alloc fail: 0
```

```
IP alias add fail: 0
```

```
Limit entry add fail: 0
```

```
NAT-Router#
```

Après avoir utilisé la commande ping 172.16.11.7 sur le routeur 4, les statistiques NAT sur le routeur 6 sont les suivantes :

```
<#root>
```

```
Router4#
```

```
ping 172.16.11.7
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router4#
```

```
NAT-Router#
```

```
show ip nat statistics
```

```
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Outside interfaces:
  GigabitEthernet1, GigabitEthernet2
Inside interfaces:
  GigabitEthernet3

Hits: 4

Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 7 pool test refcount 0
  pool test: id 1, netmask 255.255.255.0
    start 172.16.11.70 end 172.16.11.71
    type generic, total addresses 2, allocated 0 (0%), misses 0
nat-limit statistics:
  max entry: max allowed 0, used 0, missed 0
In-to-out drops: 0 Out-to-in drops: 0
Pool stats drop: 0 Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
NAT-Router#
```

Vous pouvez voir à partir des commandes show le nombre de résultats incrémentés. Dans le cas d'une requête ping réussie à partir d'un routeur Cisco, le nombre d'occurrences augmente de dix. Les échos ICMP (Internet Control Message Protocol) envoyés par le routeur source (routeur 4) sont traduits, et les paquets de réponse d'écho du routeur de destination (routeur 7) doivent également être traduits, pour un total de dix occurrences. La perte de cinq occurrences est due au fait que les réponses d'écho ne sont pas traduites ou ne sont pas envoyées à partir du routeur 7.

Ensuite, voyez si vous pouvez trouver une raison pour laquelle le routeur 7 n'envoie pas les paquets de réponse d'écho au routeur 4. À ce stade, les étapes suivantes ont été franchies :

- Le routeur 4 envoie des paquets d'écho ICMP avec l'adresse source 10.10.10.4 et l'adresse de destination 172.16.11.7.
- Une fois la NAT effectuée, le paquet reçu par le routeur 7 a l'adresse source 172.16.6.14 et l'adresse de destination 172.16.11.7.
- Le routeur 7 doit répondre à 172.16.6.14, et, puisque l'adresse 172.16.6.14 n'est pas directement connectée au routeur 7, il a besoin d'une route pour ce réseau pour pouvoir répondre.



Remarque : une autre option pour confirmer si les paquets arrivent au routeur de destination est d'utiliser une capture de paquets intégrée (EPC) ou d'utiliser un paquet debug ip icmp/debug ip avec une liste de contrôle d'accès (ACL).

Maintenant, vous devez vérifier la table de routage du routeur 7 pour vérifier si une route vers 172.16.6.14 existe :

```
<#root>
```

```
Router7#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP  
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PFR
& - replicated local route overrides by connected

Gateway of last resort is not set

```
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.16.11.0/24 is directly connected, GigabitEthernet1
L      172.16.11.7/32 is directly connected, GigabitEthernet1
Router7#
```

À partir du résultat précédent, vous pouvez observer que le routeur 7 ne possède pas de route pour le sous-réseau 172.16.6.14 dans sa table de routage. Une fois que cette erreur est corrigée et qu'une route est ajoutée à la configuration, la requête ping fonctionne. Il est utile de surveiller les statistiques NAT avec la commande `show ip nat statistics`. Cependant, dans un environnement NAT plus complexe avec plusieurs traductions, cette commande `show` n'est plus utile, et l'utilisation de `debugs` est nécessaire sur le routeur.

<#root>

Router7#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router7(config)#

```
ip route 172.16.6.0 255.255.255.0 172.16.11.6
```

Router7(config)#

end

Router7#

Router4#

```
ping 172.16.11.7
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

Router4#

NAT-Router#

```
show ip nat statistics
```

Total active translations: 2 (1 static, 1 dynamic; 1 extended)

Outside interfaces:

GigabitEthernet1, GigabitEthernet2

Inside interfaces:

GigabitEthernet3

Hits: 9

```
Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 7 pool test refcount 0
  pool test: id 1, netmask 255.255.255.0
    start 172.16.11.70 end 172.16.11.71
    type generic, total addresses 2, allocated 0 (0%), misses 0
nat-limit statistics:
  max entry: max allowed 0, used 0, missed 0
In-to-out drops: 0 Out-to-in drops: 0
Pool stats drop: 0 Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
NAT-Router#
```

Les périphériques externes au réseau ne peuvent pas communiquer avec les routeurs internes

Dans ce problème, le routeur 4 peut envoyer une requête ping aux routeurs 5 et 7, mais les périphériques du réseau 10.10.50.0 ne peuvent pas communiquer avec les routeurs 5 et 7.

<#root>

Router4#

```
ping 172.16.11.7 source 10.10.50.4
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:

Packet sent with a source address of 10.10.50.4

.....

Success rate is 0 percent (0/5)

Router4#

```
ping 172.16.6.5 source 10.10.50.4
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.6.5, timeout is 2 seconds:

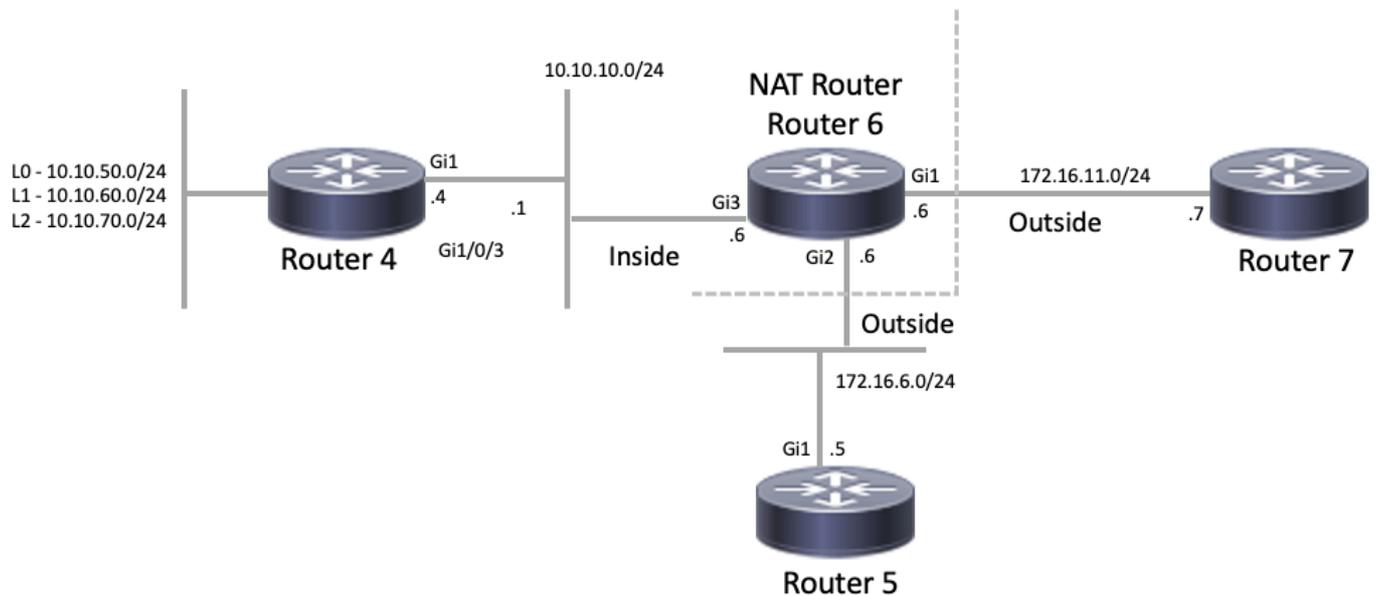
Packet sent with a source address of 10.10.50.4

.....

Success rate is 0 percent (0/5)

Router4#

Le schéma de réseau de ce problème reste le même :



Topologie NAT

<#root>

```
interface GigabitEthernet1
ip address 172.16.11.6 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
!
```

```
interface GigabitEthernet2
ip address 172.16.6.6 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
!
```

```
interface GigabitEthernet3
ip address 10.10.10.6 255.255.255.0
ip nat inside
negotiation auto
no mop enabled
no mop sysid
!
```

```
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24 ip nat inside source static 10.10.10.4 172.16.11.70
```

```
!
ip access-list standard 7
10 permit 10.10.50.4
20 permit 10.10.60.4
30 permit 10.10.70.4
```

Dépannage

À partir de la configuration du routeur 6, vous pouvez observer que la NAT est supposée traduire dynamiquement 10.10.50.4 en la première adresse disponible dans le pool NAT appelé test. Le pool se compose des adresses 172.16.11.70 et 172.16.11.71. À partir de ce problème, vous pouvez comprendre que les paquets reçus par les routeurs 5 et 7 ont l'adresse source 172.16.11.70 ou 172.16.11.71. Ces adresses se trouvent sur le même sous-réseau que le routeur 7, de sorte que le routeur 7 doit avoir une route connectée directement à ce sous-réseau. Toutefois, s'il n'en a pas déjà une, le routeur 5 a besoin d'une route vers le sous-réseau .

Vous pouvez utiliser la commande show ip route pour voir que la table de routage du routeur 5 contient l'adresse 172.16.11.0 :

```
<#root>
```

```
Router5#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

```
Gateway of last resort is not set
```

```
       172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.6.0/24 is directly connected, GigabitEthernet1
L       172.16.6.5/32 is directly connected, GigabitEthernet1

S 172.16.11.0/24 [1/0] via 172.16.6.6
```

Vous pouvez utiliser la commande show ip route pour voir que la table de routage du routeur contient l'adresse 172.16.11.0 comme sous-réseau directement connecté :

```
<#root>
```

```
Router7#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
```

- o - ODR, P - periodic downloaded static route, l - LISP
- a - application route
- + - replicated route, % - next hop override, p - overrides from PFR
- & - replicated local route overrides by connected

Gateway of last resort is not set

```

172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S      172.16.6.0/24 [1/0] via 172.16.11.6
C 172.16.11.0/24 is directly connected, GigabitEthernet1
L      172.16.11.7/32 is directly connected, GigabitEthernet1

```

Vérifiez la table de traduction NAT et assurez-vous que la traduction attendue existe. Puisque la traduction souhaitée est créée dynamiquement, vous devez d'abord envoyer le trafic IP provenant de l'adresse appropriée. Après l'envoi d'une requête ping, provenant de 10.10.50.4 et destinée à 172.16.11.7, la table de traduction du routeur 6 (routeur NAT) affiche le résultat suivant :

<#root>

NAT-Router#

show ip nat translations

```

Pro  Inside global      Inside local      Outside local      Outside global
---  172.16.6.14          10.10.10.4        ---                ---
---
172.16.11.70 10.10.50.4
---
Total number of translations: 2

```

Puisque la traduction attendue est dans la table de traduction, vous savez que les paquets d'écho ICMP sont correctement traduits. Une option est que vous pouvez surveiller les statistiques NAT, mais cela n'est pas utile dans un environnement complexe. Une autre option consiste à exécuter le débogage NAT sur le routeur NAT (routeur 6). Vous pouvez exécuter debug ip nat pendant que vous envoyez une requête ping provenant de 10.10.50.4 destinée à 172.16.11.7. Les résultats du débogage sont dans l'exemple de code suivant :

 Remarque : lorsque vous utilisez une commande debug sur un routeur, vous pouvez surcharger le routeur, ce qui le rend inutilisable. Faites toujours preuve d'une extrême prudence et, si possible, demandez l'aide d'un TAC Cisco avant d'exécuter un débogage sur un routeur de production critique.

<#root>

NAT-Router#

```
show logging
```

```
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 39 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 39 messages logged
  Trap logging: level informational, 33 message lines logged
```

```
Log Buffer (4096 bytes):
```

```
05:32:23: NAT: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [70]
05:32:23: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [70]
05:32:25: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [71]
05:32:25: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [71]
05:32:27: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [72]
05:32:27: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [72]
05:32:29: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [73]
05:32:29: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [73]
05:32:31: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [74]
05:32:31: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [74]
```

```
Router7#show monitor capture cap buffer brief
```

```
-----
# size timestamp source destination dscp protocol
-----
0 114 0.000000 172.16.11.70 -> 172.16.11.7 0 BE ICMP
1 114 2.000000 172.16.11.70 -> 172.16.11.7 0 BE ICMP
2 114 4.000000 172.16.11.70 -> 172.16.11.7 0 BE ICMP
3 114 6.001999 172.16.11.70 -> 172.16.11.7 0 BE ICMP
4 114 8.001999 172.16.11.70 -> 172.16.11.7 0 BE ICMP
```

Comme vous pouvez le voir dans la sortie de débogage précédente, la première ligne montre l'adresse source 10.10.50.4 traduite en 172.16.11.70. La deuxième ligne indique que l'adresse de destination 172.16.11.70 est retraduite en 10.10.50.4. Ce schéma se répète dans le reste du débogage. Cela signifie que le routeur NAT traduit les paquets dans les deux directions. En outre, la capture de paquets montre que le routeur 7 reçoit effectivement les paquets ICMP avec une source de 172.16.11.70 et une destination de 172.16.11.7.

Les étapes suivantes récapitulent l'état actuel de ce problème :

1. Le routeur 4 envoie un paquet provenant de 10.10.50.4 et destiné à 172.16.11.7 (ou 172.16.6.5 selon le test effectué).
2. Le routeur NAT effectue une traduction NAT sur le paquet et le transfère avec une source de 172.16.11.70 et une destination de 172.16.11.7.
3. Le routeur 7 envoie une réponse avec la source 172.16.11.7 et la destination 172.16.11.70.
4. Le routeur NAT (routeur 6) exécute la fonction NAT sur le paquet, ce qui produit un paquet avec l'adresse source 172.16.11.7 et l'adresse de destination 10.10.50.4.

5. Le routeur NAT (routeur 6) achemine le paquet vers 10.10.50.4 en fonction des informations de sa table de routage.

À ce stade, vous devez utiliser les commandes `show ip route` et `show ip cef` pour confirmer que le routeur NAT (routeur 6) a les routes nécessaires dans sa table de routage.

```
<#root>
```

```
NAT-Router#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.10.10.0/24 is directly connected, GigabitEthernet3
L    10.10.10.6/32 is directly connected, GigabitEthernet3
172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C    172.16.6.0/24 is directly connected, GigabitEthernet2
L    172.16.6.6/32 is directly connected, GigabitEthernet2
L    172.16.6.14/32 is directly connected, GigabitEthernet2
C    172.16.11.0/24 is directly connected, GigabitEthernet1
L    172.16.11.6/32 is directly connected, GigabitEthernet1
L    172.16.11.70/32 is directly connected, GigabitEthernet1
```

```
NAT-Router#
```

```
show ip route 10.10.50.4
```

```
% Subnet not in table
```

```
NAT-Router#
```

```
show ip cef 10.10.50.4
```

```
0.0.0.0/0
```

```
no route
```

```
NAT-Router#
```

Après l'ajout de la route manquante dans le routeur NAT, la requête ping aboutit :

```
<#root>
```

```
NAT-Router#
```

```
configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
NAT-Router(config)#
```

```
ip route 10.10.50.4 255.255.255.255 10.10.10.4
```

```
NAT-Router(config)#end
```

```
NAT-Router#
```

```
Router4#
```

```
ping 172.16.11.7 source 10.10.50.4
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:

Packet sent with a source address of 10.10.50.4

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

```
Router4#
```

```
ping 172.16.6.5 source 10.10.50.4
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.6.5, timeout is 2 seconds:

Packet sent with a source address of 10.10.50.4

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```
Router4#
```

Liste de vérification des problèmes courants

Utilisez cette liste de contrôle pour résoudre les problèmes courants :

Traduction non installée dans la table de traduction

Si vous constatez que la traduction appropriée n'est pas installée dans la table de traduction, vérifiez les points suivants :

1. La configuration est correcte. Il est parfois difficile d'obtenir la fonction NAT pour obtenir ce que vous voulez. Pour obtenir de l'aide sur la configuration, consultez [Configurer la traduction d'adresses réseau](#).
2. Il n'existe aucune liste d'accès entrante refusant l'entrée de paquets à partir du routeur NAT.
3. Le routeur NAT a la route appropriée dans la table de routage si le paquet passe de l'intérieur vers l'extérieur. Référez-vous à [Ordre des opérations NAT](#) pour plus d'informations.
4. La liste d'accès référencée par la commande NAT autorise tous les réseaux nécessaires.
5. Il y a assez d'adresses dans le pool NAT. Cela ne peut être un problème que si NAT n'est pas configuré pour l'encombrement.
6. Les interfaces du routeur sont convenablement définies en tant que NAT extérieure ou intérieure.
7. Pour la traduction de la charge utile des paquets DNS (Domain Name System), assurez-

vous que la traduction a lieu sur l'adresse dans l'en-tête IP du paquet. Si ceci ne se produit pas, alors la NAT ne regarde pas dans les données utiles du paquet.

La saisie de traduction correcte n'est pas utilisée

Si l'entrée de traduction correcte est installée dans la table de traduction, mais n'est pas utilisée, vérifiez :

1. Vérifiez qu'aucune liste d'accès entrante ne refuse l'entrée des paquets à partir du routeur NAT.
2. Pour les paquets qui vont de l'intérieur vers l'extérieur, vérifiez qu'il existe une route vers la destination, car elle est vérifiée avant la traduction. Référez-vous à *Ordre des opérations NAT* pour plus d'informations.

NAT fonctionne correctement, mais il reste des problèmes de connectivité

Résolvez le problème de connectivité :

1. Vérifiez la connectivité de la couche 2.
2. Vérifiez les informations de routage de la couche 3.
3. Recherchez les filtres de paquets à l'origine du problème.

%NAT System Busy - Essayer ultérieurement

Le message d'erreur `try later` apparaît quand une commande `show` associée à NAT ou une commande `show running-config` ou `write memory` est exécutée. Ceci est dû à l'augmentation de la taille de la table NAT. Quand la taille de la table NAT augmente, le routeur manque de mémoire.

1. Rechargez le routeur afin de résoudre ce problème.
2. Cette erreur se produit généralement sur les plates-formes héritées. Il est recommandé de maintenir le logiciel du périphérique à jour.

La grande table de traduction augmente la CPU

Un hôte peut envoyer des centaines de traductions, ce qui entraîne une utilisation élevée du CPU. En d'autres termes, la table peut devenir si volumineuse que la CPU fonctionne à 100 pour cent. La commande `ip nat translation max-entries 300` crée la limite 300 par hôte ou une limite agrégée du nombre de traductions sur le routeur. La solution consiste à utiliser la commande `ip nat translation max-entries all-hosts 300`.

Aucune entrée dans la table ARP

C'est le résultat de l'option `no-alias` sur les entrées NAT. L'option `no-alias` signifie que le routeur ne répond pas pour les adresses et n'installe pas d'entrée ARP. Si un autre routeur utilise un pool NAT en tant que regroupement global intérieur composé des adresses sur un sous-réseau lié, un alias est généré pour cette adresse de sorte que le routeur puisse répondre aux demandes de protocole de résolution d'adresse (ARP) de ces adresses. Ainsi le routeur dispose d'entrées ARP pour les fausses adresses.

Informations connexes

- [Traduction d'adresses réseau \(NAT\) - Forum aux questions](#)
- [Assistance et téléchargements - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.