

Vérification de l'opération NAT et dépannage

NAT de base

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Comment éliminer la cause de la NAT](#)

[Exemple de problème : peut exécuter une commande ping sur un routeur mais pas sur un autre](#)

[Résumé du problème](#)

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

[Résumé du problème](#)

[Listes de contrôle de dépannage](#)

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

[L'entrée correcte de traduction n'est pas utilisée](#)

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

[La traduction NAT pour le port 80 ne fonctionne pas](#)

[%NAT : System busy. Try later](#)

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

[%% d'adresses IP publiques déjà mappées \(adresse IP interne - > adresse IP publique\)](#)

[Aucune entrée dans la table ARP](#)

[Conclusion](#)

[Bad token 0, wanted TOK_NUMBER| TOK_PUNCT](#)

[Informations connexes](#)

[Introduction](#)

Quand vous avez des problèmes de connectivité IP dans un environnement NAT, il est souvent difficile de déterminer la cause du problème. Souvent la NAT est mise en cause à tort, quand il y a en réalité un problème fondamental. Ce document explique comment vérifier le fonctionnement de la NAT en utilisant des outils disponibles sur des routeurs Cisco. Ce document montre également comment exécuter le dépannage NAT de base et comment éviter des erreurs courantes lors du dépannage NAT.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Comment éliminer la cause de la NAT

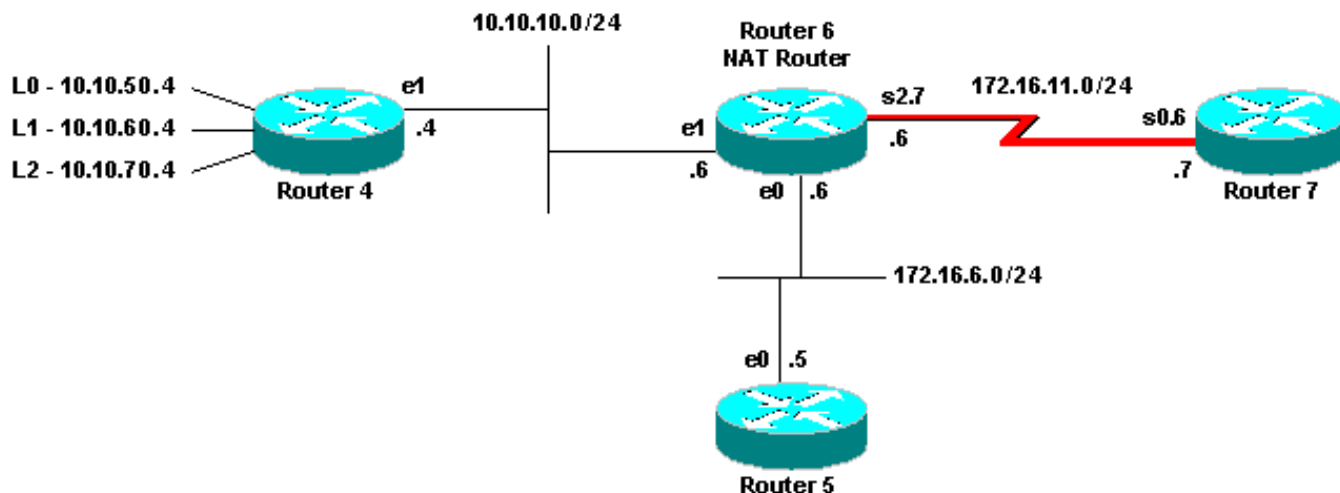
Quand vous essayez de déterminer la cause d'un problème de connectivité IP, il peut être utile de supprimer la cause de la NAT. Suivez ces étapes pour vérifier que la NAT fonctionne comme prévu :

1. Basé sur la configuration, définissez clairement ce que la NAT est censée réaliser. À cette étape vous pouvez déterminer qu'il y a un problème avec la configuration. Pour obtenir de l'aide avec la configuration de la NAT consultez la rubrique [Configuration de la traduction d'adresses réseau : Mise en route](#).
2. Vérifiez que des traductions correctes existent dans la table de traduction.
3. Utilisez les commandes **show** et **debug** pour vérifier que la traduction se produit.
4. Vérifiez en détail ce qui se passe au niveau du paquet et vérifiez que les routeurs ont les informations de routage correctes pour déplacer le paquet.

Ci-dessous se trouvent quelques exemples de problèmes dans lesquels nous avons employé les étapes ci-dessus pour déterminer la cause du problème.

Exemple de problème : peut exécuter une commande ping sur un routeur mais pas sur un autre

Dans ce schéma de réseau, le routeur 4 peut effectuer une commande ping sur le routeur 5 (172.16.6.5), mais pas le routeur 7 (172.16.11.7) :



Il n'y a aucun protocole de routage exécuté sur les routeurs, et le routeur 4 a le routeur 6 en passerelle par défaut. Le routeur 6 est configuré avec la NAT comme suit :

```

Routeur 6
interface Ethernet0
 ip address 172.16.6.6 255.255.255.0
 ip directed-broadcast
 ip nat outside
 media-type 10BaseT
 !
interface Ethernet1
 ip address 10.10.10.6 255.255.255.0
 ip nat inside
 media-type 10BaseT
 !
interface Serial2.7 point-to-point
 ip address 172.16.11.6 255.255.255.0
 ip nat outside
 frame-relay interface-dlci 101
 !
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length
24
ip nat inside source list 7 pool test
ip nat inside source static 10.10.10.4 172.16.6.14
 !
access-list 7 permit 10.10.50.4
access-list 7 permit 10.10.60.4
access-list 7 permit 10.10.70.4

```

D'abord, déterminez si la NAT fonctionne correctement. Vous savez d'après la configuration que l'adresse IP du routeur 4 (10.10.10.4) est censée être statiquement traduite 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 :

```

router-6# show ip nat translation Pro Inside global Inside local Outside local Outside global --
- 172.16.6.14 10.10.10.4 --- ---

```

Maintenant, assurez-vous que cette traduction se produit quand le routeur 4 recherche le trafic IP. Vous pouvez faire ceci de deux manières à partir du routeur 6 : en exécutant le **débugage** NAT ou en surveillant les statistiques NAT avec la commande **show ip nat statistics**. Puisque les commandes **debug** devraient toujours être utilisées en dernier recours, commencez par la commande **show**.

L'intention ici est de surveiller le compteur de résultats pour voir s'il augmente lorsque nous envoyons du trafic depuis le routeur 4. Le compteur de résultats incrémente à chaque fois qu'une traduction de la table de traduction est utilisée pour traduire une adresse. D'abord, effacez les statistiques, puis affichez les statistiques, essayez d'effectuer une commande ping du routeur 7 depuis le routeur 4, puis affichez les statistiques à nouveau.

```
router-6# clear ip nat statistics router-6# router-6# show ip nat statistics Total active translations: 1 (1 static, 0 dynamic; 0 extended) Outside interfaces: Ethernet0, Serial2.7 Inside interfaces: Ethernet1 Hits: 0 Misses: 0 Expired translations: 0 Dynamic mappings: -- Inside Source access-list 7 pool test refcount 0 pool test: 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 router-6#
```

Après avoir utilisé la commande **ping 172.16.11.7** sur le routeur 4, les statistiques NAT sur le routeur 6 indiquent que :

```
router-6# show ip nat statistics Total active translations: 1 (1 static, 0 dynamic; 0 extended) Outside interfaces: Ethernet0, Serial2.7 Inside interfaces: Ethernet1 Hits: 5 Misses: 0 Expired translations: 0 Dynamic mappings: -- Inside Source access-list 7 pool test refcount 0 pool test: 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
```

Vous pouvez voir d'après les commandes **show** que le nombre de résultats est incrémenté par cinq. Lorsqu'une commande ping provenant d'un routeur Cisco est réussie, le nombre de résultats devrait augmenter de dix. Les cinq échos d'Internet Control Message Protocol (ICMP) envoyés par le routeur d'origine (routeur 4) devraient être traduits, et les cinq paquets de réponse d'écho du routeur de destination (routeur 7) devraient également être traduits, pour un total de dix résultats. Les cinq résultats manquants correspondent très probablement aux réponses d'écho qui n'ont pas été traduites ou qui n'ont pas été envoyées du routeur 7.

Recherchez une raison pour laquelle le routeur 7 n'envoie pas de paquets de réponse d'écho au routeur 4. Vérifiez d'abord ce que la NAT fait au paquet. Le routeur 4 envoie des paquets écho ICMP avec une adresse source 10.10.10.4 et une adresse de destination 172.16.11.7. Après la NAT, le paquet reçu par le routeur 7 a une adresse source 172.16.6.14 et une 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. Contrôlez la table de routage du routeur 7 pour vérifier que la route existe.

```
router-7# show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is not set 172.16.0.0/24 is subnetted, 4 subnets C 172.16.12.0 is directly connected, Serial0.8 C 172.16.9.0 is directly connected, Serial0.5 C 172.16.11.0 is directly connected, Serial0.6 C 172.16.5.0 is directly connected, Ethernet0
```

Vous pouvez constater que la table de routage du routeur 7 ne contient pas de route pour 172.16.6.14. Une fois que vous ajoutez cette route, la commande ping fonctionne correctement.

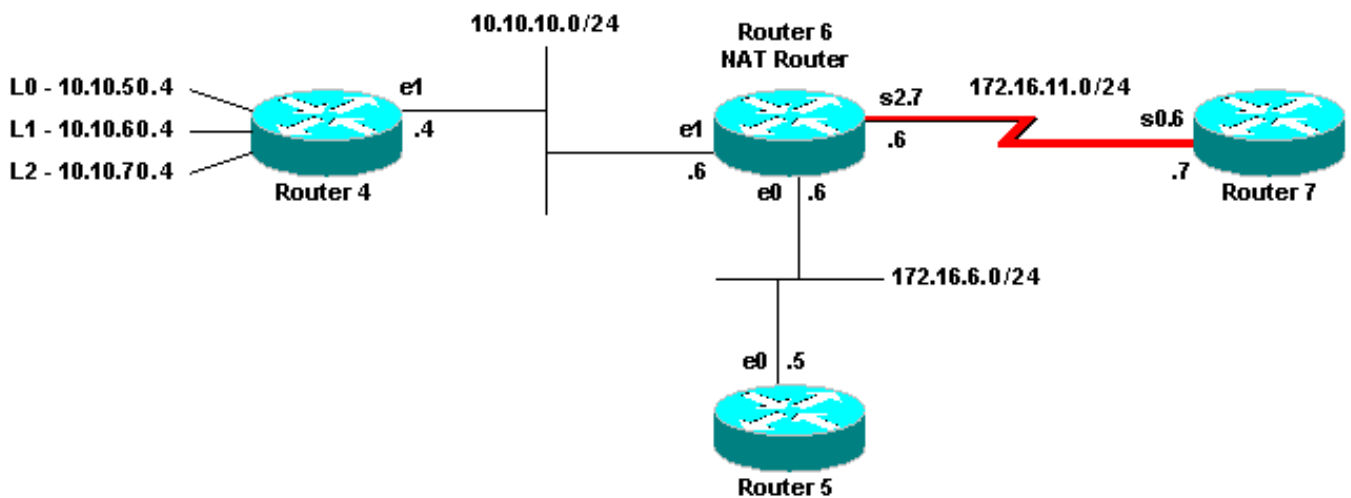
Résumé du problème

Vous avez d'abord défini ce que la NAT était censée accomplir. Ensuite, vous avez vérifié que l'entrée NAT statique existait bien dans la table de traduction et qu'elle était correcte. Vous avez vérifié que la traduction avait vraiment lieu en surveillant les statistiques NAT. Là, vous avez trouvé un problème qui vous a amené à vérifier les informations de routage sur le routeur 7, et vous avez trouvé que le routeur 7 avait besoin d'une route vers l'adresse globale interne du routeur 4.

Notez que dans cet environnement de laboratoire simple, 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. Dans ce cas, il peut être nécessaire d'exécuter des **débugages** sur le routeur. Le scénario de problème suivant explique l'utilisation des commandes **debug**.

Exemple de problème : Les périphériques externes au réseau ne peuvent pas communiquer avec les routeurs internes

Dans ce scénario, le routeur 4 peut effectuer une commande **ping** à la fois sur le routeur 5 et le routeur 7, mais les périphériques sur le réseau 10.10.50.0 ne peuvent pas communiquer avec le routeur 5 ou le routeur 7 (en laboratoire de test, nous émuloons ceci en générant des commandes **ping** depuis l'interface de bouclage avec l'adresse IP 10.10.50.4). Regardez le schéma de réseau :



Routeur 6

```
interface Ethernet0
 ip address 172.16.6.6 255.255.255.0
 ip directed-broadcast
 ip nat outside
 media-type 10BaseT
 !
interface Ethernet1
 ip address 10.10.10.6 255.255.255.0
 ip nat inside
 media-type 10BaseT
 !
interface Serial2.7 point-to-point
 ip address 172.16.11.6 255.255.255.0
 ip nat outside
 frame-relay interface-dlci 101
 !
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length
24
ip nat inside source list 7 pool test
ip nat inside source static 10.10.10.4 172.16.6.14
 !
access-list 7 permit 10.10.50.4
access-list 7 permit 10.10.60.4
access-list 7 permit 10.10.70.4
```

D'abord, énoncez clairement le comportement prévu de NAT. À partir de la configuration du routeur 6, vous savez que la NAT est censée traduire dynamiquement 10.10.50.4 en la première adresse disponible dans le pool NAT « test ». Le pool se compose des adresses 172.16.11.70 et 172.16.11.71. D'après ce que vous avez appris dans le problème ci-dessus, vous pouvez déduire que les paquets que les routeurs 5 et 7 reçoivent ont une adresse source 172.16.11.70 ou de 172.16.11.71. Ces adresses sont sur le même sous-réseau que le routeur 7, ainsi le routeur 7 devrait avoir une route directement connectée. Toutefois, le routeur 5 a besoin d'une route vers le sous-réseau s'il n'en a pas déjà.

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 :

```
router-5# show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 4 subnets C 172.16.9.0 is directly connected, Serial1 S
172.16.11.0 [1/0] via 172.16.6.6 C 172.16.6.0 is directly connected, Ethernet0 C 172.16.2.0 is
directly connected, Serial0
```

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 :

```
router-7# show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 5 subnets C 172.16.12.0 is directly connected, Serial0.8 C
172.16.9.0 is directly connected, Serial0.5 C 172.16.11.0 is directly connected, Serial0.6 C
172.16.5.0 is directly connected, Ethernet0 S 172.16.6.0 [1/0] via 172.16.11.6
```

Maintenant que vous avez clairement énoncé ce que la NAT est censée faire, vous devez vérifier que le processus fonctionne correctement. Commencez par vérifier la table de traduction NAT et vous assurer que la traduction prévue existe. Puisque la traduction qui vous intéresse est créée dynamiquement, vous devez d'abord envoyer le trafic IP provenant de l'adresse appropriée. Après l'envoi d'une commande **ping** depuis 10.10.50.4 et vers 172.16.11.7, la table de traduction du routeur 6 montre ceci :

```
router-6# show ip nat translation 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 --- ---
```

Puisque la traduction attendue est dans la table de traduction, savez-vous que les paquets d'écho ICMP sont traduits correctement, mais qu'en est-il des paquets de réponse d'écho ? Comme mentionné ci-dessus, vous pourriez contrôler les statistiques NAT, mais ce n'est pas très utile dans un environnement complexe. Une autre option consiste à exécuter le débogage NAT sur le routeur NAT (routeur 6). Dans ce cas, vous devez activer la commande **debug ip nat** sur le routeur 6 lorsque vous envoyez une commande **ping** originaire de 10.10.50.4 et destinée à 172.16.11.7. Les résultats de **débogage** sont ci-dessous.

Remarque: Quand vous utilisez n'importe quelle commande **debug** sur un routeur, vous pouvez surcharger le routeur et le rendre inopérable. Faites toujours extrêmement attention et, si possible, n'exécutez jamais une commande **debug** sur un routeur de production critique sans supervision d'un ingénieur d'assistance technique Cisco.

```
router-6# show log 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]
```

Comme vous pouvez constater d'après le résultat du **débogage** ci-dessus, la première ligne représente l'adresse source 10.10.50.4 qui est traduite en 172.16.11.70. La deuxième ligne montre l'adresse de destination 172.16.11.70 qui est retraduite en 10.10.50.4. Ce schéma se répète dans le reste du **débogage**. Ceci indique que le routeur 6 traduit les paquets dans les deux directions.

Passez maintenant en revue ce qui devrait se produire exactement. Le routeur 4 envoie un paquet de 10.10.50.4 vers 172.16.11.7. Le routeur 6 effectue la NAT sur le paquet et transfère un paquet avec une source 172.16.11.70 et une destination 172.16.11.7. Le routeur 7 envoie une réponse de 172.16.11.7 vers 172.16.11.70. Le routeur 6 effectue la NAT sur le paquet. Ainsi, le paquet a l'adresse source 172.16.11.7 et l'adresse de destination 10.10.50.4. À ce point, le routeur 6 devrait diriger le paquet vers 10.10.50.4 sur la base des informations qu'il a dans sa table de routage. Vous devez utiliser la commande **show ip route** pour confirmer que le routeur 6 dispose de la route nécessaire dans sa table de routage.

```
router-6# show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 5 subnets C 172.16.8.0 is directly connected, Serial1 C
172.16.10.0 is directly connected, Serial2.8 C 172.16.11.0 is directly connected, Serial2.7 C
172.16.6.0 is directly connected, Ethernet0 C 172.16.7.0 is directly connected, Serial0
10.0.0.0/24 is subnetted, 1 subnets C 10.10.10.0 is directly connected, Ethernet1
```

Résumé du problème

Vous avez d'abord clairement défini ce que la NAT était censée accomplir. En second lieu, vous avez vérifié que les traductions nécessaires existaient dans la table de traduction. Troisièmement, vous avez utilisé les commandes **debug** ou **show** pour vérifier que la traduction avait réellement lieu. Enfin, vous avez minutieusement passé en revue ce qui arrivait au paquet et ce dont les routeurs avaient besoin pour transférer le paquet ou y répondre.

Listes de contrôle de dépannage

Maintenant que vous avez une procédure de base pour rechercher la cause des problèmes de connectivité, voici quelques listes de contrôle pour dépanner des problèmes fréquents.

Traduction non installée dans la table de traduction

Si vous constatez que la traduction appropriée ne s'installe pas dans la table de traduction, vérifiez les points suivants :

- La configuration est correcte. L'obtention des résultats escomptés de la NAT peut parfois être délicat. Pour obtenir de l'aide pour la configuration, consultez la rubrique [Configuration de la traduction d'adresses réseau : Mise en route](#).

- Il n'existe pas de liste d'accès en entrée qui refuse les paquets entrant sur le routeur NAT.
- Le routeur NAT dispose de la route appropriée dans la table de routage si le paquet va de l'intérieur à l'extérieur. Référez-vous à [Ordre des opérations NAT](#) pour plus d'informations.
- La liste d'accès référencée par la commande NAT autorise tous les réseaux nécessaires.
- Il y a assez d'adresses dans le pool NAT. Ceci devrait être un problème seulement si la NAT n'est pas configurée pour la surcharge.
- Les interfaces du routeur sont convenablement définies en tant que NAT extérieure ou intérieure.
- Dans le cas de la traduction des données utiles des paquets de Système de noms de domaine (DNS), 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.

[L'entrée correcte de traduction n'est pas utilisée](#)

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

- Il n'existe pas de liste d'accès en entrée qui refuse les paquets entrant sur le routeur NAT.
- Pour les paquets allant de l'intérieur à l'extérieur, la destination dispose d'une route comme vérifié avant la traduction. Référez-vous à [Ordre des opérations NAT](#) pour plus d'informations.

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

Si la NAT fonctionne correctement, commencez le dépannage du problème de connectivité comme suit :

- Vérifiez la connectivité de la couche 2.
- Vérifiez les informations de routage de la couche 3.
- Recherchez des filtres de paquet qui pourraient être la cause du problème.

[La traduction NAT pour le port 80 ne fonctionne pas](#)

La traduction NAT pour le port 80 ne fonctionne pas, mais la traduction pour les autres ports fonctionne normalement.

Pour résoudre ce problème, exécutez les étapes suivantes :

1. Exécutez les commandes **debug ip nat translations** et **debug ip packet** pour vérifier si les traductions sont correctes et si l'entrée de traduction correcte est installée dans la table de traduction.
2. Vérifiez que le serveur répond.
3. Désactivez le serveur HTTP.
4. Effacez les tables de NAT et ARP.

[%NAT : System busy. Try later](#)

Le message d'erreur %NAT: [System busy](#). Try later apparaît quand une commande **show** associée

à une NAT ou une commande **show running-config** ou **write memory** est exécutée. Ce problème 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.

Rechargez le routeur afin de résoudre ce problème. Si le message d'erreur apparaît quand le HSRP SNAT est configuré, configurez ces commandes afin de résoudre le problème :

```
Router(config)#standby delay minimum 20 reload 20
Router(config)#standby 2 preempt delay minimum 20 reload 20 sync 10
```

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

Un hôte peut envoyer des centaines de traductions, qui mènent à leur tour à l'utilisation importante de la 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** établit la limite de 300 par hôte ou la limite agrégée de la quantité de traductions sur le routeur. La solution consiste à utiliser la commande **ip nat translation max-entries all-hosts 300**.

[%% d'adresses IP publiques déjà mappées \(adresse IP interne - > adresse IP publique\)](#)

Ce message apparaît quand vous essayez de configurer deux adresses IP internes à une adresse IP publique écoutant les mêmes ports.

```
% X.X.X.X already mapped (172.30.62.101 -> X.X.X.X)
```

Pour effectuer une NAT de l'adresse IP publique pour deux adresses IP internes, utilisez deux adresses IP publiques dans le DNS.

[Aucune entrée dans la table ARP](#)

C'est le résultat de l'option *no-alias* qui est utilisé sur les entrées NAT. L'option *no-alias* signifie que le routeur ne répond pas pour les adresses et n'installe pas une 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.

[Conclusion](#)

Les problèmes ci-dessus prouvent que la NAT n'est pas toujours la cause des problèmes de connectivité IP. Dans de nombreux cas, la cause des problèmes n'est pas la NAT et des recherches approfondies doivent être effectuées. Ce document explique des étapes de base du dépannage et de la vérification de l'opération NAT. Ces étapes incluent les suivantes :

- Définir clairement ce que la NAT est censée réaliser.
- Vérifier que la table de traduction contient bien les traductions correctes.
- Utilisez les commandes **show** et **debug** pour vérifier que la traduction se produit.
- Vérifiez en détail ce qui se passe au niveau du paquet et vérifiez que les routeurs ont les informations de routage correctes pour déplacer le paquet.

[Bad token 0, wanted TOK NUMBER|TOK PUNCT](#)

Ce message d'erreur est juste un message d'information et n'a pas d'incidence sur le comportement normal du périphérique.

```
Bad token 0, wanted TOK_NUMBER|TOK_PUNCT
```

L'erreur signifie que la NAT tente de corriger la couche 4 sur l'adresse dans un FTP ouvert et qu'elle ne trouve pas les adresses IP dont elle a besoin pour traduire dans le paquet.

La raison pour laquelle le message inclut des jetons est que les adresses IP dans le paquet sont trouvées en recherchant un jeton, ou un ensemble de symboles, dans le paquet IP, afin de rechercher les détails requis pour effectuer la traduction.

Quand une session FTP est initiée, elle négocie deux canaux, un canal de commande et un canal de transmission de données. Ce sont deux adresses IP avec différents numéros de port. Le client FTP et le serveur négocient un deuxième canal de transmission de données pour transférer des fichiers. Le paquet échangé via le canal de contrôle a le format « PORT,i,i,i,i,p,p », où i,i,i,i, représente les quatre octets d'une adresse IP et p, p représente le port. La NAT tente d'appliquer ce schéma et de traduire l'adresse/le port si nécessaire. La NAT doit traduire les deux schémas d'adressage des deux canaux. La NAT recherche des numéros dans le flux de commande jusqu'à ce qu'elle pense avoir trouvé un commande de port qui requiert une traduction. Elle essaye d'analyser la traduction, qu'elle calcule grâce au schéma décrit plus tôt.

Si le paquet est corrompu ou si le serveur FTP ou le client a des commandes malforming, la NAT ne peut pas correctement calculer la traduction et elle génère cette erreur. Nous vous suggérons de définir le client FTP sur « passif » de sorte qu'il lance les deux canaux. Cette solution est parfois utile pour le FTP via NAT.

[Informations connexes](#)

- [Page de support NAT](#)
- [Support technique - Cisco Systems](#)